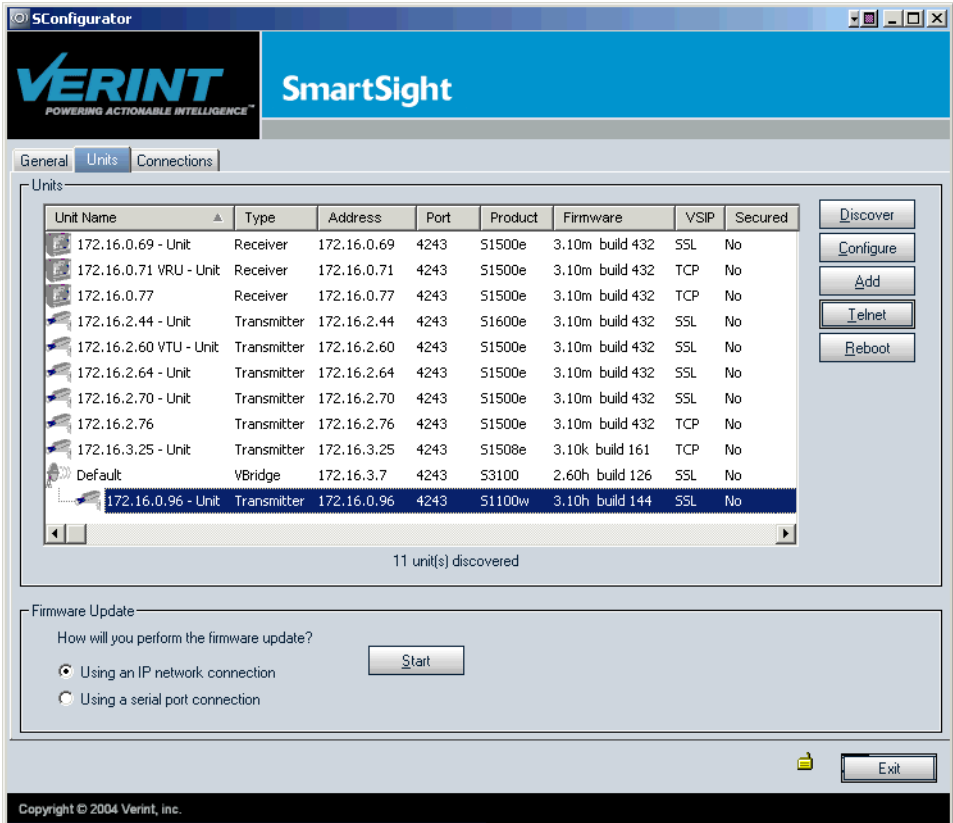


# SConfigurator User Manual





# **SConfigurator**

**Software Release 4.0**

# **User Manual**

**Verint Video Solutions**

© 2005 Verint Systems Inc. All rights reserved.

By providing this document, Verint Systems Inc. is not making any representations regarding the correctness or completeness of its contents and reserves the right to alter this document at any time without notice.

Verint, Actionable Intelligence, BehaviorTrack, Dellis, HealthCheck, Lanex, Loronix, Loronix Video Manager, MotionTrack, microDVR, nDVR, netDVR, Nextiva, Powering Actionable Intelligence, SmartSight, and Video Manager are trademarks of Verint Systems Inc., its subsidiaries or affiliates. All other registered trademarks, trademarks, and any associated logos are the properties of their respective owners.

Published by:

Verint Video Solutions  
1800 Berlier Street  
Laval (Quebec)  
Canada  
H7L 4S4  
[www.verint.com/videosolutions](http://www.verint.com/videosolutions)

Publication date: April 21, 2005

# Contents

<b>Preface .....</b>	<b>v</b>
About SConfigurator .....	vi
Who Should Read this Manual .....	vi
How to Use this Manual .....	vii
Contents .....	vii
Conventions .....	viii
Related Documentation .....	viii
Related Nextiva Products .....	ix
About Us .....	ix
<b>Chapter 1 ■ Getting Started .....</b>	<b>1</b>
Computer Requirements .....	2
Starting SConfigurator .....	2
Changing SConfigurator Settings .....	3
IP Network .....	4
SSL .....	6
<b>Chapter 2 ■ Setting Up the Edge Devices .....</b>	<b>9</b>
Discovering Edge Devices .....	10
Choosing Information to Display .....	14
Configuring a Device .....	15
General Status .....	17
Network\Ethernet .....	19
Network\VSIP .....	20
Network\SSL .....	21
Network\NTP .....	22
Network\Wireless .....	23
Network\Wireless\Link Status .....	31
Network\Filters .....	33
Video .....	34
Video\Input .....	34
Video\Input\Encoder .....	35
Video Decoder .....	40
Serial Port .....	40
Audio .....	42
Audio\Encoder .....	43
Audio\Decoder .....	44
Performing a Batch Network Configuration .....	45

**Chapter 3 ■ Updating Firmware ..... 47**  
    Performing the Update .....48  
    Firmware Update Messages .....51

**Chapter 4 ■ Enabling Security ..... 53**  
    Building a Secure System .....54  
    Establishing the Default Secure VSIP Connection .....55  
    Adding a Device to the Trusted List .....56

**Chapter 5 ■ Troubleshooting an Edge Device ..... 57**

**Chapter 6 ■ Managing Connections ..... 61**  
    Adding a Connection .....62  
    Removing a Connection .....64

**Chapter 7 ■ Accessing the CLI ..... 65**  
    SConfigurator Console .....66  
    Telnet .....68

**Chapter 8 ■ Aligning the Antenna ..... 69**

**Appendix A ■ DHCP Support and APIPA Service..... 71**

**Glossary ..... 73**

**Index ..... 81**

# Preface

The *SConfigurator User Manual* presents the information and procedures for configuring Nextiva™ edge devices:

- Wired video servers:
  - S1500e series covering the S1500e, S1502e, S1504e, and S1508e
  - S1600e
  - S1700e series
  - S1708e series covering the S1708e, S1712e, and S1724e
- IP cameras—S2500e
- Wireless video servers—S1000w and S1100w
- Outdoor wireless bridge—S3100

# About SConfigurator

SConfigurator is a PC-based administration tool for use over any TCP/IP network. SConfigurator is built on open standards to provide long-term investment protection.

You use SConfigurator to:

- Configure Nextiva edge devices
- Add security in your system
- Get information on the devices connected on the network
- Connect video servers together
- Update the firmware of the devices
- Align the antennas of wireless devices

SConfigurator is shipped on the *SmartSight Utilities* CD.

## Who Should Read this Manual

This manual is intended for IT system administrators, engineers, and technicians who will configure and manage the Nextiva edge devices. It provides conceptual information on how to use the SConfigurator software.

This manual assumes that you are familiar with:

- General use of computers
- Microsoft Windows operating systems
- Local area networks (LANs) and basic IP data communication concepts and practices



# How to Use this Manual

This manual contains all the information needed to configure and manage Nextiva video servers and outdoor wireless bridges.

## Contents

The *SConfigurator User Manual* is divided into the following chapters:

1. **Getting Started**—Explains how to start SConfigurator and change its settings.
2. **Setting Up the Edge Devices**—Presents the procedures for configuring the Nextiva edge devices.
3. **Updating Firmware**—Describes the procedures for updating the firmware of the Nextiva edge devices.
4. **Enabling Security**—Explains how to secure communication between SConfigurator and the edge devices.
5. **Troubleshooting an Edge Device**—Includes a series of frequently asked questions on device configuration.
6. **Managing Connections**—Explains how to create or remove connections between transmitter and receiver video servers.
7. **Accessing the CLI**—Describes the ways to access the command line interface of the edge devices.
8. **Aligning the Antenna**—Explains how to align the antenna of a wireless device with that of its master bridge.

The manual also includes the following appendix:

- A **DHCP Support and APIPA Service**—Explains how the dynamic host configuration protocol server and the Microsoft APIPA service work.

A glossary and an index complete the manual.

# Conventions

The following typographic conventions are used throughout this manual:

Visual cue	Meaning
<b>Connect</b>	The name of an interface element you have to act on. A key to press. The value of an interface element.
<b>Advanced &gt; VSIP</b>	Any sequence of steps (in the menu structure of a graphical application, in the navigation structure of a web site, and so on).
<i>connection_name</i>	Text that must be replaced by a user-supplied value. Text representing variable content.
S3100.zzh	The name of a command, file, or directory. Text that appears on the screen. Examples of user-supplied values.

## Related Documentation

In addition to this manual, the following documentation is also available on the *SmartSight Utilities* CD shipped with the edge devices:

- *S1000w Series User Manual*—Contains conceptual information on the configuration, installation, and operation of the S1000w devices.
- *S1100w User Manual*—Contains conceptual information on the configuration, installation, and operation of the S1100w devices.
- *S1500e Series User Manual*—Contains conceptual information on the configuration, installation, and operation of the S1500e series devices.
- *S1600e User Manual*—Contains conceptual information on the configuration, installation, and operation of the S1600e devices.
- *S1700e Series User Manual*—Contains conceptual information on the configuration, installation, and operation of the S1700e series devices.

- *S1708e Series User Manual*—Contains conceptual information on the configuration, installation, and operation of the S1708e series devices.
- *S2500e User Manual*—Contains conceptual information on the configuration, installation, and operation of the S2500e IP cameras.
- *S3100 User Manual*—Contains conceptual information on the configuration, installation, and operation of the S3100 outdoor wireless bridges.
- *Release Notes*—Contain information about SConfigurator upgrades and known issues still under investigation, as well as a description of features not covered in this version of the documentation.

## Related Nextiva Products

The S1000w, S1100w, S1500e series, S1700e series, S1708e series, S2500e, and S3100 edge devices can be used with the nDVR™ and Nextiva software packages from Verint Video Solutions. For more details about these packages, visit our web site. For pricing information, call your dealer.

## About Us

Verint Systems (NASDAQ: VRNT) is a leading global provider of video security, surveillance and business intelligence solutions. Verint Video Solutions transform digital video into actionable intelligence: timely, mission-critical insights for faster, more effective decisions.

Today, more than 1000 companies in 50 countries use Verint Systems solutions to enhance security, boost operational efficiency, and fuel profitability.

## Web Site

For information about the Nextiva line of products, visit [www.verint.com/videosolutions](http://www.verint.com/videosolutions).

To download application notes and user documentation, as well as request the latest versions of firmware and software, you need access to the Verint Video Solutions partner extranet. To register, go to [www.verint.com/smartsight/support](http://www.verint.com/smartsight/support).

The data sheets of the edge devices are also available directly at [www.verint.com/smartsight/support](http://www.verint.com/smartsight/support).

## Support

If you encounter any type of problem after reading this manual, contact your local distributor or Verint Video Solutions representative. You can also use the following sections on the Verint Video Solutions partner extranet web site to find the answers to your questions:

- SmartSight FAQ
- SmartSight Requests
- SmartSight My Account

Verint Video Solutions technical support personnel is available to help you use your Nextiva edge devices and the related software:

- By phone: 1 888 494-7337 (North America) or  
+1 450 686-9000 Monday to Friday, from 8:30 to  
17:30 EST
- By fax: +1 450 686-0198

# 1

## Getting Started

Before using SConfigurator to configure Nextiva edge devices, you need to set parameters for the IP network and for SSL (Secure Sockets Layer) security.

# Computer Requirements

The minimum software and hardware requirements for the computer needed to use SConfigurator are:

- Windows 2000 Service Pack 2 or higher, or Windows XP
- An Ethernet network card
- A serial port (not through a USB converter)

## Starting SConfigurator

The SConfigurator tool is part of the *SmartSight Utilities* CD. For the latest version of the tool, visit the Verint Video Solutions web site (Firmware Upgrades section).

### To start SConfigurator:

1. Each time you have a new software version, copy the SConfigurator.exe file to the hard disk of your computer.
2. In the Windows file manager, start the SConfigurator.exe program.

The SConfigurator window appears.



The SConfigurator main window has three tabs:

Tab	Description
General	To change SConfigurator options, to enter the command line interface (CLI), and to align the antennas of wireless devices
Units	To get an inventory of the Nextiva edge devices on the IP network, to configure them, and to perform firmware updates
Connections	To manage the point-to-point connections between video servers

## Changing SConfigurator Settings

Program options allow you to set SConfigurator parameters relative to the IP network and to SSL.

The screenshot shows the 'Program Options' dialog box with the following fields and controls:

- IP Address of the PC :** A dropdown menu showing '192.168.135.222'.
- Detect All Units on LAN :** An unchecked checkbox.
- VSIP Port :** A text box containing '5510', with 'Default' and 'Common' buttons to its right.
- Discovery IP Address :** A text box containing '255 . 255 . 255 . 255', with 'Reset to Broadcast' and 'Reset to Multicast' buttons below it.
- SSL Section:**
  - Trusted Unit List :** A text box with a 'Browse' button to its right.
  - Enable Security:** An unchecked checkbox.
  - Enter SSL Passkey :** A button located below the 'Enable Security' checkbox.
- Buttons:** 'OK' and 'Cancel' buttons at the bottom of the dialog.

## IP Network

The following SConfigurator settings are mainly used to discover Nextiva devices on the IP network; for more information about the discovery process, see page 10. The settings are:

- IP Address of the PC—The unique IP address of the computer where SConfigurator runs. You do not normally have to change this value, since SConfigurator automatically detects it. However, you can change the displayed value if:
  - You are using two Ethernet cards on your PC.
  - You are using a virtual private network (VPN).
  - The IP address of the computer has changed.
- Detect All Units on LAN—The indication of whether all devices connected to the same LAN as the PC and having the same VSIP port as SConfigurator will be discovered, even those whose IP addresses are not part of the same subnet as the computer.

*Note: This setting works only with the broadcast detection method. If you select it, SConfigurator automatically switches to broadcast, even if the Discovery IP Address field displays the multicast address.*

You typically activate this setting to discover the new devices on the network and those in APIPA mode (for more information about APIPA, see page 71). When it is activated, device discovery will take more time.



- **VSIP Port**—The communication port used for VSIP (video services over IP) command-and-control messaging between SConfigurator and Nextiva devices. You have to set the port number to the same value in SConfigurator and in the devices to be configured. The default VSIP port is 5510.

*Note: VSIP ports 9541, 65500, and those under 1024 are reserved and should never be used, not even for serial port, video, or audio communication.*

Furthermore, all devices and SConfigurator have the ability to receive messages on a hard-coded VSIP port, 9541, called the *common* port.

Unless otherwise specified, the phrase *VSIP port* refers to the configurable port and not to the common port.

- **Discovery IP Address**—The communication method and associated IP address SConfigurator will use to detect Nextiva devices on the network. Contact your system administrator to know which method your network supports. Possible methods are:
  - **Broadcast**—Sending a message to all devices physically connected to the same network as SConfigurator; it may not reach devices on other LANs. The broadcast IP address is 255.255.255.255. (Default)
  - **Multicast**—Sending a message to a selected group of devices. With the multicast method, SConfigurator can discover devices located across multiple networks, but not through the Internet. The current multicast IP address is 224.16.32.1 and should not be changed.

## To change the SConfigurator IP network settings:

1. In the General tab, click **Program Options**.

The Program Options window appears.

IP Address of the PC : 192.168.135.222

Detect All Units on LAN : ☐

VSIP Port : 5510 Default Common

Discovery IP Address : 255 . 255 . 255 . 255

Reset to Broadcast Reset to Multicast

## 1: Getting Started

2. If required, change the IP address of the computer and the detection scope.
3. To change the configurable VSIP port, do one of the following steps:
  - In the VSIP Port field, type its new value.
  - To reset it to its default value, click **Default**.
  - To set it to the common value, click **Common**.
4. To set the discovery IP address, click **Reset to Broadcast** or **Reset to Multicast** depending on your supported discovery method.
5. Click **OK**.

## SSL

You can enable the SSL protocol between SConfigurator and Nextiva devices. This way, VSIP communication occurring on the IP network will be secure. For more information about SSL, see the “Enabling Security” chapter on page 53.

By default, SConfigurator can communicate with devices holding an SSL certificate (*SSL-enabled* devices) as well as non-SSL devices. However, you can increase security by forcing SConfigurator to communicate only with SSL-enabled devices that it trusts and that share the same SSL passkey.

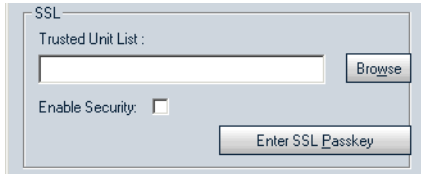
The SConfigurator SSL settings are:

- **Trusted Unit List**—The list of trusted Nextiva devices that SConfigurator will manage in a secure system.
- **Enable Security**—The indication of whether SConfigurator can communicate only with SSL-enabled devices that are included in the trusted list and that share the same SSL passkey.
- **Enter SSL Passkey**—To change the password shared by SConfigurator and SSL-enabled devices to establish a secure VSIP connection.

**To change the SConfigurator SSL settings:**

- 1.** In the General tab, click **Program Options**.

The Program Options window appears.



- 2.** To create the trusted unit list:
  - a.** In the SSL box, click **Browse**.
  - b.** Choose the directory that will hold the list.
  - c.** In the **File name** field, enter a meaningful name, then click **Open**.

The path and name of the list appear in the Trusted Unit List field.

- 3.** To change the trusted unit list, click **Browse**, then select the desired file.
- 4.** To force SConfigurator to communicate only with SSL-enabled devices that are part of the trusted list, check **Enable Security**.
- 5.** To change the SSL passkey:
  - a.** Click **Enter SSL Passkey**.

The SSL Passkey window appears.

- b.** Type the passkey, then click **OK**.

You will need to enter this passkey each time you start SConfigurator in security-enabled mode.

- 6.** Click **OK**.



# 2

## Setting Up the Edge Devices

You can perform the following tasks in the Units tab of the SConfigurator window:

- Discovering edge devices on the network
- Choosing information to display
- Configuring edge devices
- Performing a batch network configuration

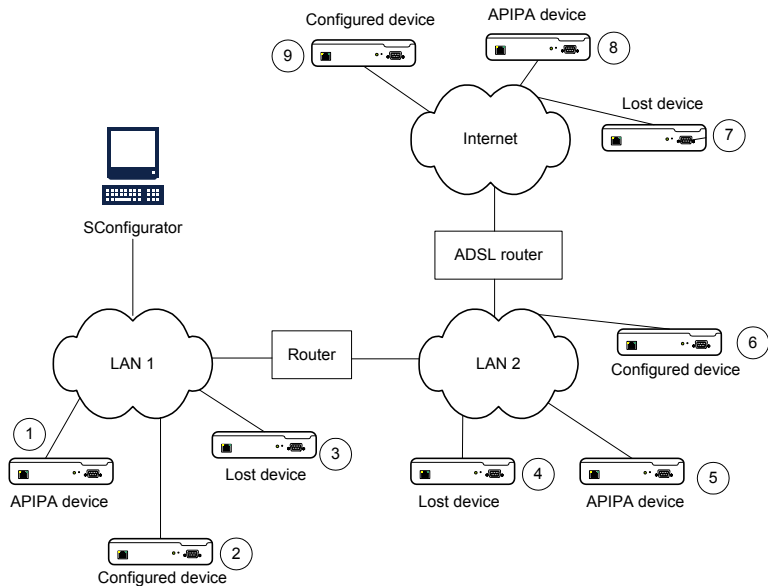
# Discovering Edge Devices

The Units tab displays the devices that have been discovered by SConfigurator on the IP network. The number of devices found varies depending on the following settings (which are part of the program options described on page 4):

- The communication method used to detect devices on the network
- The VSIP port
- The Detect All Units on LAN setting

Regardless of the number of devices to discover, you should take into account the SSL security status in SConfigurator (described on page 6).

To present the discovery scenarios, consider the following network configuration:



Three types of devices (which can be wired or wireless video servers, or outdoor wireless bridges) are presented:

- A properly configured device having the same VSIP port as SConfigurator (*Configured device*)

- A device in APIPA mode: A brand new device, a device having been through a factory reset, a device with a duplicate IP address, or a device unable to receive an address from a DHCP server (*APIPA device*)

For more information about APIPA, see page 71.

- A device whose VSIP port and IP address are unknown (*Lost device*)

The following discovery scenarios are available:

Scenario	Broadcast	Multicast	Unicast	Common VSIP port	Detect All Units on LAN	Discovered devices
A	✓					2
B	✓				✓	1, 2
C	✓			✓		2, 3
D	✓			✓	✓	1, 2, 3
E		✓			n/a	2, 6
F		✓		✓	n/a	2, 3, 4, 6
G			✓		n/a	2, 6, 9
H			✓	✓	n/a	2, 3, 4, 6, 7, 9

The scenarios with the broadcast method are:

- SConfigurator can find devices only on the local network, provided they share the same VSIP port (device 2).
- The Detect All Units on LAN setting works only in broadcast mode. This setting helps detect the APIPA device (device 1), which resides on a subnet different from that of the computer. Their VSIP ports need to be the same.
- The common port is required to find the lost device (device 3), since its configured VSIP port is different from SConfigurator's.

## 2: Setting Up the Edge Devices

The scenarios with the multicast method are:

- SConfigurator can locate devices attached to remote networks (device 6, provided they share the same VSIP port), but not through the Internet.
- SConfigurator cannot find the APIPA devices (devices 1 and 5), since they require the Detect All Units on LAN setting available only with the broadcast method.
- The common port helps locate the lost devices (devices 3 and 4).

The scenarios with the unicast method are:

- Each device is discovered individually. Typically, you use unicast when the device cannot be located with the broadcast or multicast methods.
- SConfigurator can detect all devices sharing the same VSIP port, even those accessible only through Internet (device 9), provided you know their individual IP addresses.
- SConfigurator cannot locate the APIPA devices (devices 1, 5, and 8) since they require the Detect All Units on LAN setting available only with the broadcast method.
- The common port helps locate the lost devices (devices 3, 4, and 7).

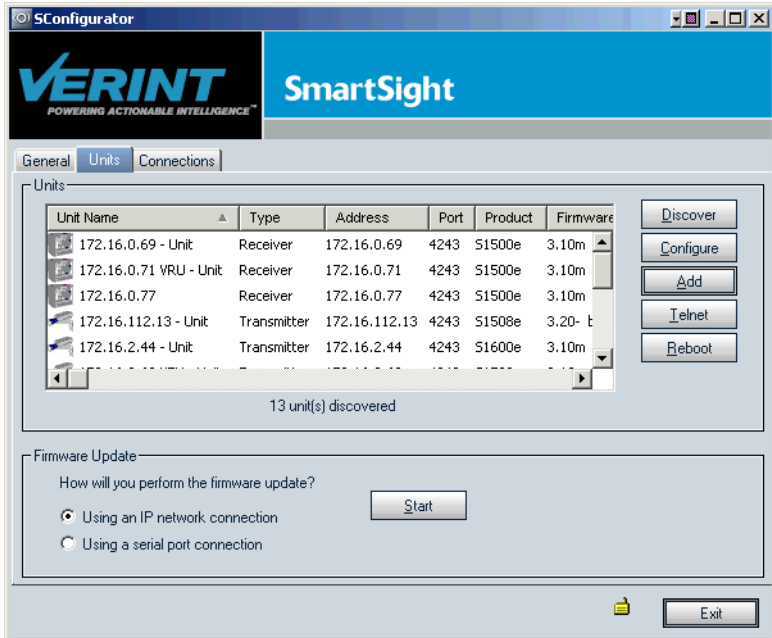
In the Units tab, you use the **Discover** button to find many devices with the broadcast or multicast method (depending on the Discovery IP Address setting in the program options). To discover a single device with the unicast method, you use the **Add** function. Be aware however that most unicast-discovered devices will disappear from the Units box the next time you click **Discover**, since the list is emptied before the broadcast or multicast command is launched.



## To discover devices with the broadcast or multicast method:

- ◆ In the Units tab, click **Discover**.

The discovered devices appear in the Units box.

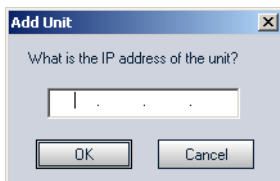


If *unknown* devices appear, see the probable causes in the “Troubleshooting an Edge Device” chapter on page 57.

## To find a specific device with the unicast method:

1. In the Units tab, click **Add**.

The Add Unit window appears.



2. Enter the IP address of the device you want to find, then click **OK**.

The device is added to the Units box.

# Choosing Information to Display

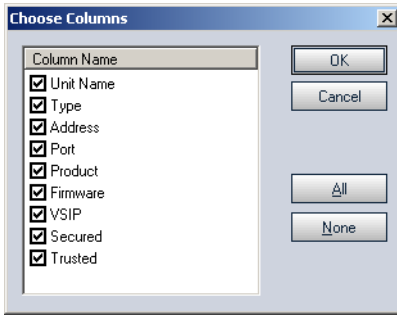
You can select the columns that will appear in the Units box. The available columns are:

- **Unit Name**—A meaningful name given to the device in the System Status tab.
- **Type**—The function of the device. Possible values are: Receiver, Transmitter, and VBridge.
- **Address**—The IP address of the device.
- **Port**—The configurable VSIP port of the device.
- **Product**—The type of the Nextiva device (for example, S1100w, S1500e, S3100, and so on).
- **Firmware**—The version of the firmware in the device.
- **VSIP**—The type of VSIP connection between the device and SConfigurator. Possible values are:
  - **UDP**—A connection type used for point-to-multipoint messaging. It is not used anymore and remains for backward compatibility only.
  - **TCP**—An error-free connection (default).
  - **SSL**—A TCP connection secured with SSL.
- **Secured**—The indication of whether the Enable Security option is enabled in the device.
- **Trusted**—The indication of whether the device is part of the trusted list (for more information, see page 6).

**To choose the information to display:**

1. In the Units box, right-click any device.
2. From the contextual menu, choose **Choose Columns**.

The Choose Columns window appears.



3. Select the desired columns, then click **OK**.

## Configuring a Device

SConfigurator allows you to change or display several settings for the devices:

Setting	S1500e series, S1600e, S1700e series, S1708e series	S1000w, S1100w	S2500e	S3100
General	✓	✓	✓	✓
Network				
Ethernet, VSIP, SSL, NTP	✓	✓	✓	✓
Wireless		✓		✓
Filters				✓
Link status				✓
Video encoder	-T	✓		
Video decoder	-R			
Serial port	✓	✓		
Audio	optional	✓		

## 2: Setting Up the Edge Devices

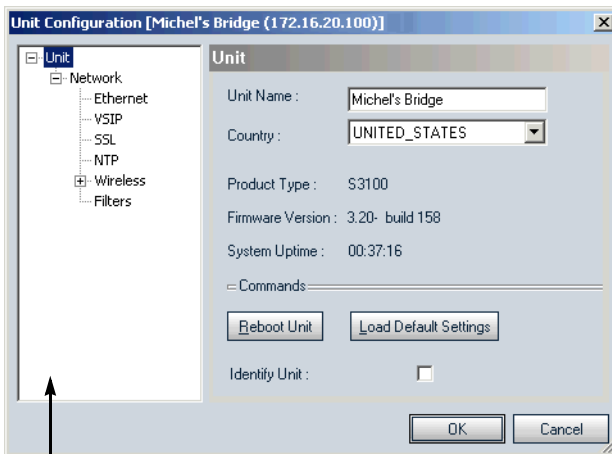
Since the S1500e series, S1700e series, S1708e series, S2500e, and S1100w devices are mainly used with a video management software (rather than in point-to-point connections), you should not configure them entirely with SConfigurator, since their settings will be overwritten in the software. In this context, only the initial configuration (for the wired devices) and the wireless settings (for the S1100w) should be performed with SConfigurator.

The S1100 devices are not specifically covered, since you will use the SmartSight Configuration Assistant tool to configure them. However, you may have to use SConfigurator to change their wireless settings when the devices are part of a repeater setup.

### To access the configuration parameters:

1. In the Units box, double-click the desired device.

A Unit Configuration window appears.



**Parameter tree**

2. In the parameter tree, click the desired category, then make the necessary changes. You may have to expand a category name by clicking the plus (+) sign to its left.
3. Click **OK**.

Each time you change one or more settings then click **OK**, a confirmation window appears. After you confirm the changes, the device may reboot.

# General Status

At the root of the parameter tree, in the Unit pane, you find system status information on the device: type, firmware version, and uptime.

Also, you can change the following parameters:

- For the S1100w and S3100 devices, you may have to set the country of operation. Depending on the country, the available frequency bands may differ and the DFS (Dynamic Frequency Selection) and TPC (Transmit Power Control) regulations may apply.

For more information about these regulations, refer to the user manual of the device.

- You should assign a meaningful name to every device. This name will be displayed in the Units box, under the Unit Name column.

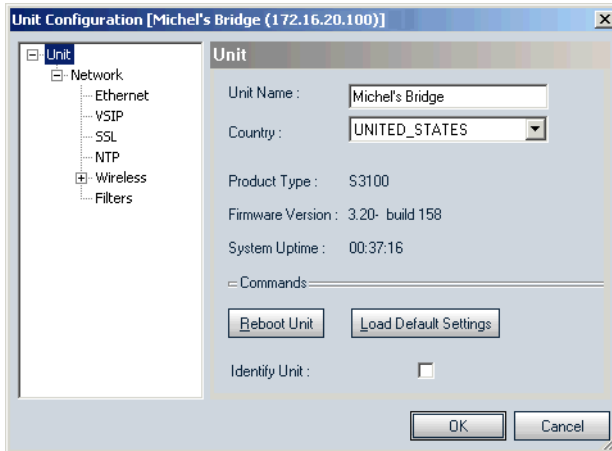
Furthermore, the Unit pane allows you to execute the following operations:

- Identify the device—Makes the status LED of the device flash red rapidly to recognize it among a large set of devices.
- Reboot the device—Performs a warm boot of the device. This operation will keep the current device configuration.
- Load default settings—Resets all configuration parameters to their factory settings. For a list of these settings, refer to the "Factory Default Configuration" appendix in the user manual of the device.

## 2: Setting Up the Edge Devices

### To access the general settings:

1. In the parameter tree, click **Unit**.



2. To change the name of the device, enter a meaningful name in the Unit Name field.
3. If required, select the country of operation of the device.
4. To reboot the device or load its default settings:
  - a. Click **Reboot Unit** or **Load Default Settings** respectively.

A confirmation message appears.
  - b. Click **Yes**.
5. To identify the device:
  - a. Check **Identify Unit**.

The status LED flashes red.
  - b. To reset the LED to its previous state, clear **Identify Unit**.
6. Click **OK**.

# Network\Ethernet

The Network\Ethernet pane allows you to set a series of IP network parameters:

- **Use DHCP**—The indication of whether a DHCP (dynamic host configuration protocol) server will be used to provide a valid network configuration for your device. For details on DHCP support, see Appendix A on page 71.

DHCP takes care of the IP address, subnet mask, and gateway information.

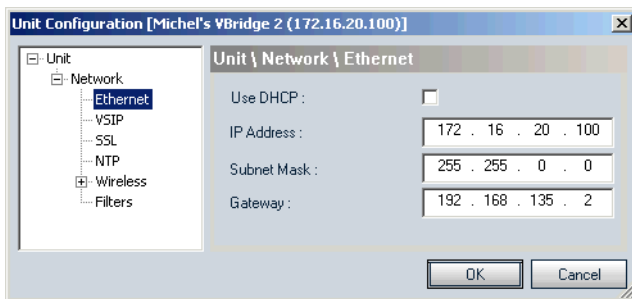
- **IP Address**—The unique 32-bit IP address of the device.
- **Subnet Mask**—The binary configuration specifying in which subnet the IP address of the device belongs. A subnet is a portion of a network that shares a common address component. Unless otherwise specified by your network administrator, it is recommended that you use a subnet mask of 255.255.255.0.
- **Gateway**—The IP address of your gateway. A gateway represents a network point that acts as an entrance to another network. Contact your network administrator for the correct gateway information.

*Warning: Never use the IP address of the device as the gateway value.*

You can perform a batch network configuration if you have many devices to configure. For the procedure, see page 45.

## To change the Ethernet network settings:

1. In the parameter tree, expand the **Network** structure, then click **Ethernet**.



## 2: Setting Up the Edge Devices

2. Change the desired settings.
3. Click **OK**.

# Network\VSIP

The Network\VSIP pane contains the parameters related to the VSIP (video services over IP) protocol. The values of these parameters must be the same in the device and in SConfigurator. For more information about the available discovery methods, see page 5.

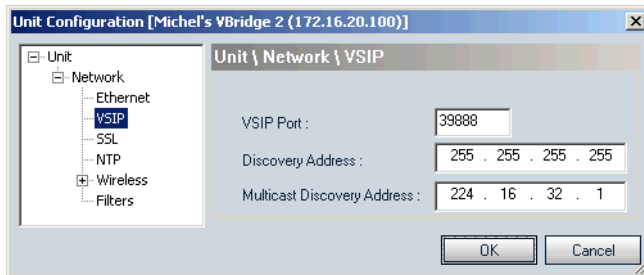
- VSIP Port—The VSIP port used by the device to communicate with SConfigurator. The default value of all Nextiva devices is 5510.

*Note: VSIP ports 9541, 65500, and those under 1024 are reserved and should not be used, not even for serial port, video, or audio communication.*

- Discovery Address—The IP address used by the device to make its presence known to SConfigurator with the broadcast method. The broadcast address is 255.255.255.255.
- Multicast Discovery Address—The IP address used by the device to make its presence known to SConfigurator with the multicast method. The current multicast address is 224.16.32.1 and should not be changed.

### To change the VSIP settings:

1. In the parameter tree, expand the **Network** structure, then click **VSIP**.



2. Change the desired settings.
3. Click **OK**.



# Network\SSL

On devices with an SSL digital certificate, you can enable security so that they will only accept secure VSIP connections. Once a device is in secure mode, you cannot access it anymore with Telnet, you cannot perform firmware updates through the IP network on it, and its access through the web interface (for the S1600e, S1700e, and S2500e devices).

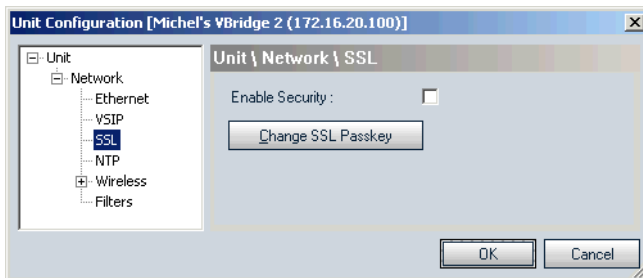
To enable SSL security on the device, the parameters are:

- **Enable Security**—The indication of whether the device only accepts SSL VSIP connections.
- **Change SSL Passkey**—To change the password shared by SConfigurator and all SSL-enabled devices to establish a secure system. You can change it only if the connection between the device and SConfigurator is secure.

For more information about SSL, see the “Enabling Security” chapter on page 53.

## To change the SSL settings:

1. In the parameter tree, expand the **Network** structure, then click **SSL**.



2. To change the SSL passkey:
  - a. Click **Change SSL Passkey**.
3. To restrict the device to secure connections only, check **Enable Security**.

The SSL Passkey window appears.

- b. Type the passkey, then click **OK**.

After its reboot, the device will accept only SSL VSIP connections.

4. Click **OK**.

## Network\NTP

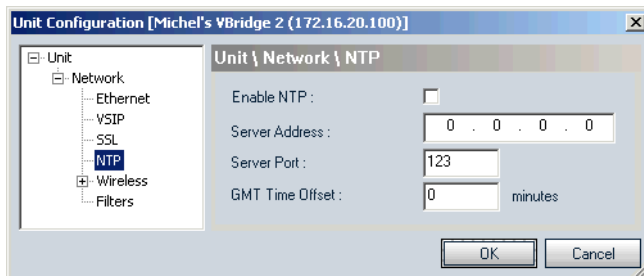
The video server can connect to a Network Time Protocol (NTP) server to get the current time. The main reason to use NTP is to display valid dates in the log files instead of the device uptime. NTP uses GMT (Greenwich Mean Time) to synchronize device clock time.

The NTP parameters are:

- Enable NTP—The indication of whether NTP is used.
- Server Address—The IP address of the NTP server.
- Server Port—The IP port of the NTP server.
- GMT Time Offset—The offset (in minutes) from GMT in the current time zone.

### To change the NTP settings:

1. In the parameter tree, expand the **Network** structure, then click **NTP**.



2. Change the desired settings.
3. Click **OK**.

## Network\Wireless

The Network\Wireless pane appears only on wireless transmitters (S1100w, S1100, and S1000w) and outdoor bridges (S3100).

In a wireless setup, the order in which you configure the devices (either the first time or later when they are installed in the field) is critical if you do not want to lose access to them. For more information about this specific order or about the wireless parameters described next, refer to the user manual of the Nextiva device.

### S1100w, S1100, and S3100 Devices

The wireless settings for the S1100w, S1100, and S3100 devices are:

- **Mode**—The MAC (media access control) mode of the device. Possible values are:
  - SDCF—For point-to-point applications
  - SPCF—For point-to-multipoint systems and in repeater contexts

The available MAC modes vary depending on the devices:

  - S1100 and S1100w—The only possible mode is SPCF.
  - S3100—Both modes are available. SPCF is the default.
- **Role**—The function of the device in the wireless system.
  - S1100 and S1100w—The only available role is **Client**.
  - S3100—Possible values are: **Master** (default) and **Slave**.
- **Band**—The RF (radio frequency) band used by the device. The possible values are:
  - 802.11a—5 GHz OFDM
  - 802.11g—2.4 GHz OFDM

- **Channel**—The frequency channel, within the selected band, that the wireless system will use.

- **Master S3100**—If your devices are operating in a DFS environment, you cannot manually select the frequency channel; in this context, the displayed value of the Channel parameter is **Auto**.

On a master bridge in a non-DFS environment, you can choose the RF channel that will be used by the wireless cell or the automatic channel selection.

The channels available in North America are:

- 1 to 11 in the 2.4 GHz band
- 52, 56, 60, and 64 in the 5.3 GHz band
- 149, 153, 157, 161, and 165 in the 5.8 GHz band

To know which channels are available elsewhere, refer to the *Wireless Frequency Plan* document located on our web site (Tools & Demos section).

- **S1100, S1100w, and slave S3100**—Even though the channel is assigned by the connected master S3100, you can specify an initial value for the *roaming* process by which the device will find its bridge. However, this initial channel may not be the one used by the bridge.
- **Bit Rate**—The transmission data rate at which the device operates. This parameter is available on S1100, S1100w, and S3100 slave devices.

Possible values are:

- **Auto**—The best possible value (with a default RF margin of 15 dB) automatically assigned when the device connects to its wireless bridge. To change the margin, see page 26.
- 6, 9, 12, 18, 24, 36, 48, and 54 Mbps.

Once the device is operating properly, Verint Video Solutions strongly recommends to change the configured bit rate from Auto to the actual bit rate of the connection (for the procedure, see page 32).

- **Starting Order**—A sequence number, used during the boot-up process of a master device in a DFS context, to delay its startup. The purpose of this parameter is to ensure that colocated master devices will not start at the same time. The default starting order is 1. Every colocated cell should have a different starting order: It should be incremented by 1 in each system.

The starting order is available only in master devices and has an impact only when the channel selection is automatic.

- **Antenna Gain**—The gain of the antenna on the device (in dBi). If you use an external antenna with your device, it is important to enter its gain in SConfigurator. This way, the device will be able to automatically change its transmission power so that the total power (device and antenna) does not exceed the maximum value established by your country's regulations.

- **Transmission Power**—The indication of the level of emitting power of the device radio. The available values are:

- ☐ **Maximum**—The maximum allowed.
- ☐ **50%**—The power is reduced by 3 dB.
- ☐ **25%**—The power is reduced by 6 dB.
- ☐ **12.5%**—The power is reduced by 9 dB.
- ☐ **Minimum**—The power is set at 3 dBm.

By default, the transmission power of a device subject to the TPC regulations is set to 50%.

- **Maximum Distance**—In SDCF mode, the maximum transmission distance (between a master and slave S3100) in all wireless cells present in the same geographical region and sharing the same frequency channel. The two S3100 devices making up an SDCF wireless cell must have the same value for this parameter.

## 2: Setting Up the Edge Devices

- **Sensitivity Threshold**—The minimum signal level perceived by the radio of the device. The default value is **Normal**.

Reducing the sensitivity of the radio enables unwanted “noise” to be filtered out. A safe value is 10 dB below the current received signal level (displayed in the Network\Wireless\Link Status pane of the associated S3100). The default value represents the most sensitive context. You must be careful not to reduce the sensitivity to a level where the device would not “hear” its legitimate correspondent.

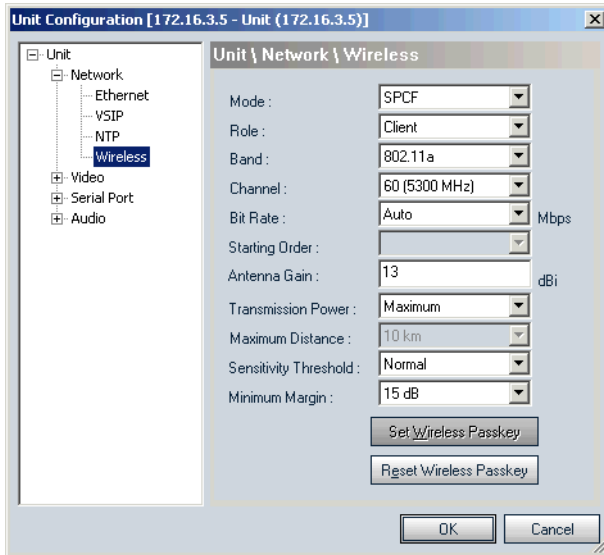
- **Minimum Margin**—The minimum RF margin used when the transmission bit rate is set to Auto. It represents the difference in dB between the actual signal received by the device and the minimum signal required by a given bit rate to correctly receive data on the RF link. The default minimum margin is 15 dB.

This parameter is available on S1100, S1100w, and S3100 slave devices.

In addition to these radio frequency parameters, the S1100w, S1100, and S3100 devices have a *wireless passkey*, a unique identifier enabling secure and encrypted RF communication with their outdoor wireless bridges. This key is made up of either 32 hexadecimal digits or 16 text characters and is case sensitive. You can either provide a value for the passkey or reset it to its default factory value.

**To change the wireless settings for an S1100w or S1100 device:**

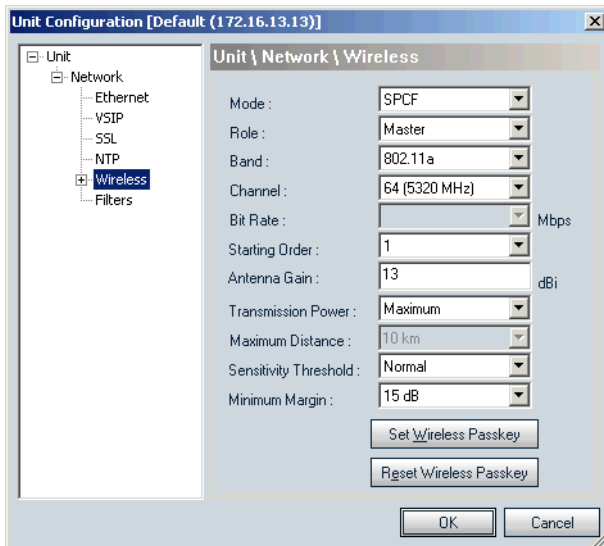
1. In the parameter tree, expand the **Network** structure, then click **Wireless**.



2. Change the settings as required.
3. Click **OK**.

**To set the wireless settings for a master bridge:**

1. In the parameter tree, expand the **Network** structure, then click **Wireless**.



2. Ensure that the Role field contains **Master**.
3. In SDCF mode, set the value of the Maximum Distance field.
4. Change the other settings as required.
5. Click **OK**.

**To set the wireless settings for a slave bridge:**

1. In the parameter tree, expand the **Network** structure, then click **Wireless**.

2. In the Role field, select **Slave**.

3. Click **OK** to save the settings.

The device reboots.

4. In the Units tab, click **Discover**.

5. Select the slave device, then click **Configure**.

6. In the parameter tree, expand the **Network** structure, then click **Wireless**.



7. Change the other settings as required.
8. Click **OK**.

### To change the wireless passkey:

*Note: You can change this passkey only if the connection is secure between the device and SConfigurator; for the procedure, see Chapter 4 on page 53.*

1. In the Wireless pane, click **Set Wireless Passkey**.

The Set Wireless Passkey window appears.

2. Select the format of the passkey.
3. In the Passkey field, enter the new passkey.

For the wireless connection to be secure, do not enter a known name (like a street name), but instead use a mix of digits and letters. Furthermore, do not disclose the passkey.

4. In the Confirmation field, enter again the passkey.
5. To apply the new password to all associated devices on a master bridge:
  - a. Ensure that **Apply Changes to Connected Clients/Slaves** is checked.
  - b. Click **OK**.

*Note: The wireless passkey of the S3100 device will be changed only when you click **OK** in the Unit Configuration window.*

The Changing Wireless Passkey window appears.

- c. When the procedure is finished, click **Close**.

6. On an S1100w, S1100, or slave bridge, clear **Apply Changes to Connected Clients/Slaves**, then click **OK**.
7. To set the wireless passkey to its default value, click **Reset Wireless Passkey** in the Wireless pane.
8. Click **OK**.

## S1000w Devices

The wireless settings for the S1000w devices are:

- **Channel**—The frequency channel that will be used by the device. Eleven channels are available: 1 to 11.
- **Bit Rate**—The data rate at which the device operates. A high bit rate reduces the effective distance between two functional devices.

The bit rate can be set to 1, 2, 5.5, or 11 Mbps. The recommended bit rate is 2 Mbps for all system installations unless the link is unreliable; in this case, use 1 Mbps, which will slightly reduce the video frame rate.

- **SSID**—The service set identifier, a name for a pair of devices (transmitter and receiver) working together; the SSID must be the same for both devices. Collocated systems must always be set on different SSIDs. The SSID is represented by an ASCII string of 1 to 32 characters (number or letters).
- **Change WEP Key**—To change the WEP (wired equivalent privacy) key of the device. The WEP encryption mechanism provides protection from eavesdropping using another S1000w device or a computer equipped with a wireless 802.1 receiver. The WEP key is used by the device to generate a unique encryption sequence. It must be the same for a transmitter and a receiver connected together.

The WEP key can have two formats (text and hexadecimal) and two encryption types (64-bit and 128-bit). The number of digits forming the key varies depending on these settings:

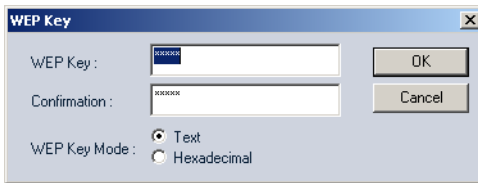
	Text	Hexadecimal
<b>64-bit</b>	5 printable ASCII characters	10 digits (0-9; a-e; A-E)
<b>128-bit</b>	13 printable ASCII characters	26 digits (0-9; a-e; A-E)

- WEP—The indication of whether WEP encryption is activated. If encryption is disabled, the system will still offer some level of protection through the unique SSID.

### To change the wireless settings for an S1000w device:

1. In the parameter tree, expand the **Network** structure, then click **Wireless**.
2. In the Channel, Bit Rate, and SSID fields, change the desired settings as required.
3. To change the WEP key:
  - a. Click **Change WEP Key**.

The WEP Key window appears.



- b. Select the WEP key mode.
  - c. In the WEP Key field, enter the new key.
  - d. In the Confirmation field, re-enter the key.
  - e. Click **OK**.
4. To activate the WEP key, select **Active** in the WEP list.
5. Click **OK**.

## Network\Wireless\Link Status

The Network\Wireless\Link Status pane contains information on the devices (client or slave) connected to a master S3100:

- IP Address—The IP address of the device.
- Unit Name—The name of the device.
- Unit Rx Bit Rate—The reception data rate (in Mbps) of the client or slave. It corresponds to the transmission bit rate of the master.
- Unit Rx Level—The average signal level (in dBm) indicating the strength of the signal received by the client or slave.

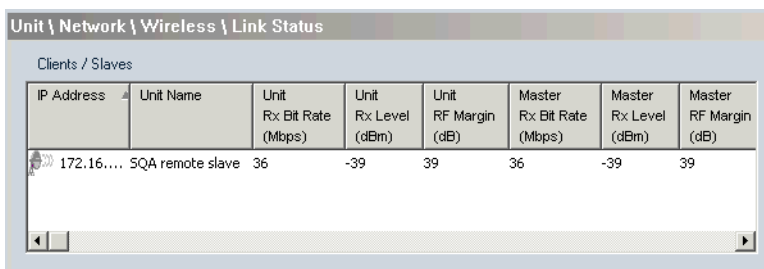
## 2: Setting Up the Edge Devices

- **Unit RF Margin**—The RF margin (in dB) used by the client or slave.
- **Master Rx Bit Rate**—The reception data rate (in Mbps) of the master. It corresponds to the transmission bit rate of the client or slave. You can manually change this value.
- **Master Rx Level**—The average signal level (in dBm) indicating the strength of the signal received by the master.
- **Master RF Margin**—The RF margin (in dB) used by the master.

Once a client or slave device is operating properly, Verint Video Solutions strongly recommends to change its configured bit rate from the default value to the actual bit rate of the connection. This way, the wireless communication will be more stable in the presence of changing atmospheric conditions or other RF interferers. If the quality of the RF link degrades severely, the actual bit rate could be lower than the manually configured one.

### To change the transmission bit rate of a client or slave:

1. In the parameter tree of the master device, expand the **Network** and the **Wireless** structures, then click **Link Status**.



The screenshot shows a software window titled "Unit \ Network \ Wireless \ Link Status". Below the title bar is a tab labeled "Clients / Slaves". The main area contains a table with 8 columns: IP Address, Unit Name, Unit Rx Bit Rate (Mbps), Unit Rx Level (dBm), Unit RF Margin (dB), Master Rx Bit Rate (Mbps), Master Rx Level (dBm), and Master RF Margin (dB). A single row of data is visible, representing a device with IP address 172.16.1.100, named "SQA remote slave". The values for this device are: Unit Rx Bit Rate: 36, Unit Rx Level: -39, Unit RF Margin: 39, Master Rx Bit Rate: 36, Master Rx Level: -39, and Master RF Margin: 39.

IP Address	Unit Name	Unit Rx Bit Rate (Mbps)	Unit Rx Level (dBm)	Unit RF Margin (dB)	Master Rx Bit Rate (Mbps)	Master Rx Level (dBm)	Master RF Margin (dB)
172.16.1.100	SQA remote slave	36	-39	39	36	-39	39

2. In the Clients/Slaves list, right-click the desired device, then choose **Force Transmission Bit Rate**.

3. In the **Desired Bit Rate** field of the Force Transmission Bit Rate window, select the new value, then click **OK**.

The device reboots. The new bit rate is then displayed in the list.

*Note: You cannot change the bit rate of the same device a second time without leaving the Unit Configuration window, re-discover the devices, then access the configuration settings of the master bridge.*

## Network\Filters

The Network\Filters pane contains the settings for controlling the flow of data between the wireless and wired Ethernet networks. These settings are not taken into account for broadcast communication.

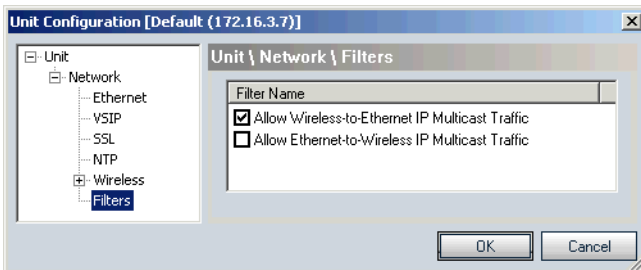
The available filters allowing multicast traffic are:

- From the wireless to the wired network
- From the wired to the wireless network

By default, wireless-to-wired traffic is enabled, allowing data to flow from wireless transmitters to receivers on the wired network (either Nextiva video receivers or computers running a video management software).

### To change the filter setting:

1. In the parameter tree, expand the **Network** structure, then click **Filters**.



2. Select the desired filters.
3. Click **OK**.

## Video

The Video structure in the parameter tree enables you to properly configure the video on transmitter devices.

The only setting applicable to the complete video functionality is:

- **Standard**—The analog display standard. Two standards are supported: PAL and NTSC.

### To change the video standard:

1. In the parameter tree, click **Video**.



2. Change the setting.
3. Click **OK**.

## Video\Input

The number of video inputs varies depending on the device.

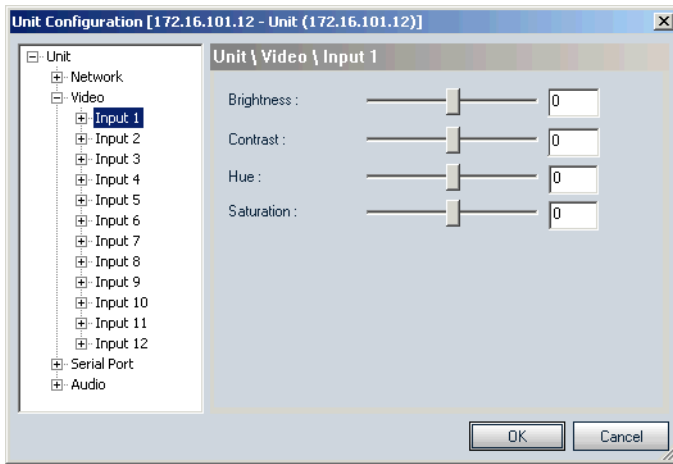
A series of parameters relative to the treatment of colors is available for each video input:

- **Brightness**—The total amount of light in a color. The values range from -128 (no brightness) to 127 (white).
- **Contrast**—The range of colors in the image. The values range from -128 (luminance off) to 127; 0 is the CCIR level. Increasing the contrast of a color palette makes different colors easier to distinguish, while reducing the contrast makes them appear washed out.
- **Hue**—The relative amounts of red, green, and blue in a color. The values range from -180 (-180d) to 179 (179d); 0 is 0d. Hue corresponds to the common definition of color, for example, "red," "orange," and "violet."

- **Saturation**—The vividness of a color, the intensity of the colors in the image. The values range from -128 (color off) to 127; 0 is the CCIR level.

### To change the video input settings:

1. In the parameter tree, expand the **Video** structure, then click the desired **Input**.



2. Change the desired settings.
3. Click **OK**.

## Video\Input\Encoder

The number of encoders varies depending on the number of video inputs in the device:

- On the S1500e series, S1600e, S1700e series, S1708e, S1712e, and S2500e devices, the incoming video for each input is duplicated and sent to two separate encoders (numbered 1 and 2).
- On the S1724e, each video input has only one activated encoder.
- The S1000w and S1100w devices have a single input; typically, only one encoder is available for the input. To enable the second video encoder, call Verint Video Solutions technical support.

## 2: Setting Up the Edge Devices

You can use different applications on each video encoder. Here are typical contexts using the video management software packages and the web interface:

Device	Input 1		Input 2		...
	Encoder 1	Encoder 2	Encoder 1	Encoder 2	
S1000w, S1100w	point to point	n/a	n/a	n/a	
	software: view at rate A	n/a	n/a	n/a	
S1500e	point to point	n/a	n/a	n/a	
	software: view at rate A	software: archive at rate B	n/a	n/a	
S1502e	point to point	n/a	point to point	n/a	
	software: view at rate A	software: archive at rate B	software: view at rate A	software: archive at rate B	
S1504e, S1508e	software: view at rate A	software: archive at rate B	software: view at rate A	software: archive at rate B	...
S1600e	web viewing	point to point	n/a	n/a	
S1700e, S2500e	web viewing	point to point	n/a	n/a	
	point to point	n/a	n/a	n/a	
	software: view at rate A	software: archive at rate B	n/a	n/a	
S1708e, S1712e	software: view at rate A	software: archive at rate B	software: view at rate A	software: archive at rate B	...
S1724e	software: view at rate A	n/a	software: view at rate A	n/a	...

If using more than one encoder, you need more bandwidth.

You can change the following settings:

- **Target Bit Rate**—The maximum number of bits per second generated by the device. Valid bit rates range from 10 to 4000 kbps. This value depends on many variables, like network capacity and the number of devices sending data on the network.



- **Target Frame Rate**—The maximum number of frames per seconds (fps) that will be encoded and transferred by the transmitter. This parameter can be set to 1 to 7, 10, 15, or 30 fps in NTSC mode and 1 to 6, 8, 12, or 25 fps in PAL mode.
- **Maximum Quantizer**—A parameter related to video quality. The value range is from 2 to 31. To maintain the video frame rate (that is, not to skip any frames), you should set the quantizer to 31. If the quality of each frame is more important, you should reduce the quantizer value. For example, a maximum quantizer of 5 keeps a good image quality, but skips frames when motion is high.
- **Intra Interval**—The frequency at which a complete video frame (called *I-frame*) is sent by the encoder. Possible values are in the 0–1000 range. A value of 0 indicates that no I-frame will be sent; a value of X means that a complete image refresh will occur every X frames.
- **Rate Control**—The mode controlling the bit rate variation. The following modes are available:
  - **Constant Bit Rate**—This mode is the most effective to maintain the target bit rate. Video quality may suffer and the frame rate may decrease. This mode should be used when transmitting video over networks that have very limited bandwidths, and with an intra interval value of 0 (default).
  - **Advanced Constant Bit Rate**—This mode maintains the target bit rate but is less precise than the constant bit rate. Video quality may suffer and the frame rate may decrease. This mode is preferred for high frame rate contexts.
 

*Note: This mode is not available on the S1700e series, S1708e series, and S2500e devices.*
  - **Constant Frame Rate**—This mode maintains the target frame rate. Video quality may suffer and the bit rate may exceed the target value.
- **Resolution**—The number of pixels (columns \* lines) for each picture of the video sequence. A high resolution increases picture quality but at the price of raising the bit rate. For example, the 2CIF and 4CIF modes should not be used with a bandwidth of less than 1000 kbps.

## 2: Setting Up the Edge Devices

Here are the available resolutions:

Resolution	Number of columns		Number of lines		Device
	NTSC	PAL	NTSC	PAL	
QCIF	176		128	144	All devices except S1000w and the S1708e series
CIF	352		240	288	All devices
2CIF	352		384	448	Versions prior to 3.10: All devices except S1502e and S1508e Version 3.10: All devices Version 4.0 and up: All devices except S1700e series and S2500e
2CIFH	704		240	288	Versions 2.60 and up: All devices except S1000w
4CIF	704		480	576	Versions prior to 3.10: All devices except S1502e and S1508e Version 3.10: All devices
All lines	352		480	576	Versions 2.50 up to 2.60: All devices except S1000w, S1502e, and S1508e Version 3.10 and up: All devices except S1000w
2/3D1	480		480	576	Version 3.10 and up: All devices except S1000w
VGA	640		480	576	Version 3.10 and up: All devices except S1000w

### ■ Encoder Mode—The way the video encoder works.

*Note: This setting is not used by transmitters with firmware version 2.60 or higher.*

Possible values are:

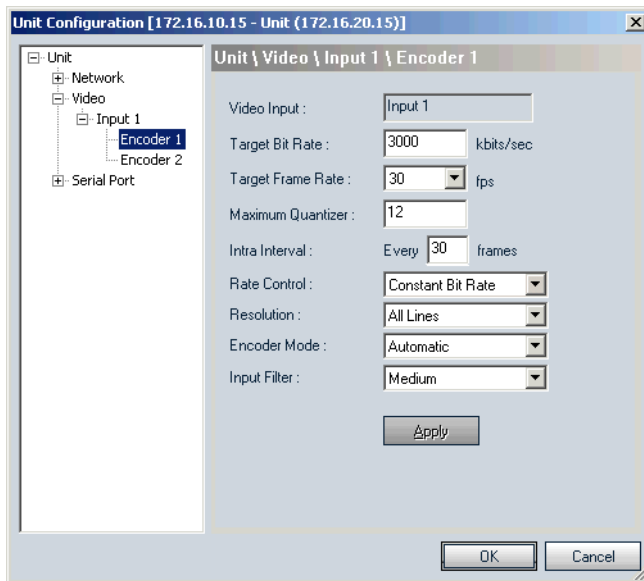
- Automatic—The device switches between the two other modes depending on the bit rate, the frame rate, and the resolution (default).
- Quality—The encoder is optimized to produce the best possible quality, to the detriment of the frame rate.

- High Frame Rate—The encoder is optimized to maintain 25–30 fps. Use this mode in high resolution (2CIF) and high frame rate (25–30 fps).
- Input Filter—The level of filtering applied to the video signal before it is encoded, helping to remove high frequency noise from lower quality cameras or noisy video feeds. The default value is **Medium**.

In removing noise from the video signal, the filter also reduces the sharpness of the image. If the signal is relatively clean, use a setting of **None** to avoid losing crispness. For images with too much noise, applying the filter can help clean up the image. Keep in mind however that the higher the filter level, the blurrier the video image may become.

### To change the video encoder settings:

1. In the parameter tree, expand the **Video** and the desired **Input** structures, then click the desired **Encoder**.



2. Change the desired settings.
3. To immediately see the changes on the monitor (except for **Rate Control** and **Resolution**) without saving them, click **Apply**.

## 2: Setting Up the Edge Devices

4. Click **OK**.

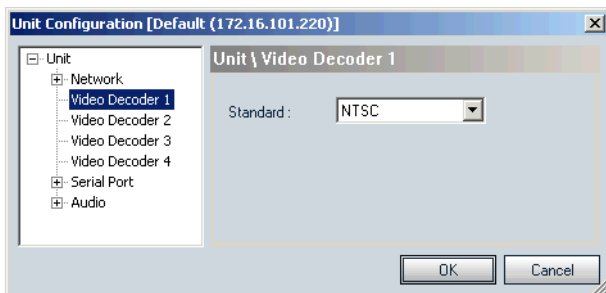
# Video Decoder

The Video Decoder pane enables you to properly configure the standard (PAL or NTSC) on receiver video servers.

The number of video outputs varies depending on the device.

### To change the video decoder setting:

1. In the parameter tree, click the desired **Video Decoder**.



2. If required, change the setting.
3. Click **OK**.

# Serial Port

The Serial Port structure in the parameter tree allows you to specify how the device will communicate with the serial equipment (dome, keyboard, matrix, multiplexer, or access card).

The hierarchy in the parameter tree varies depending on the device:

Device	Number of serial ports	Type of serial port
S1000w, S1100w	1	Either RS-232 or RS-422/485 (auto-detected)
S1500e series, S1600e, S1700e series, S1708e series	2	RS-232 and RS-422/485 ports

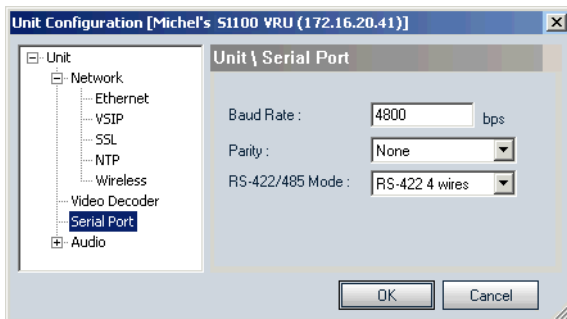
The serial port settings are:

- **Baud Rate**—The data rate that the serial equipment operates at. Possible values range from 1200 bps to 230,400 bps (transmitters) or to 115,200 bps (receivers).
- **Parity**—Odd, even, or no parity check. Most communication devices do not use parity.
- **RS-422/485 Mode**—The way the RS-422/485 serial equipment will interface with the Nextiva device. The supported operating modes are: **RS-422 4 wires**, **RS-485 2 wires**, and **RS-485 4 wires**. Obviously, this setting only applies to an RS-422/485 port.

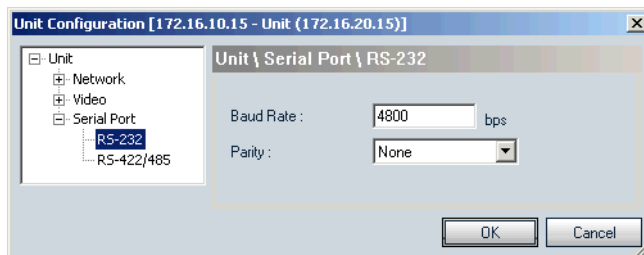
For more information about these settings, refer to the serial equipment documentation or contact your product manufacturer.

### To change the serial port settings:

1. For an S1000w or S1100w device, click **Serial Port** in the parameter tree.



2. For an S1500e series, S1600e, S1700e series, and S1708e series device, expand the **Serial Port** structure, then click the desired serial port.



## 2: Setting Up the Edge Devices

3. Change the desired settings.
4. Click **OK**.

# Audio

The Audio structure in the parameter tree enables you to properly configure the audio on transmitter or receiver devices. It appears in the parameter tree only if audio is supported on your video server.

The number of audio encoders and decoders varies depending on the device.

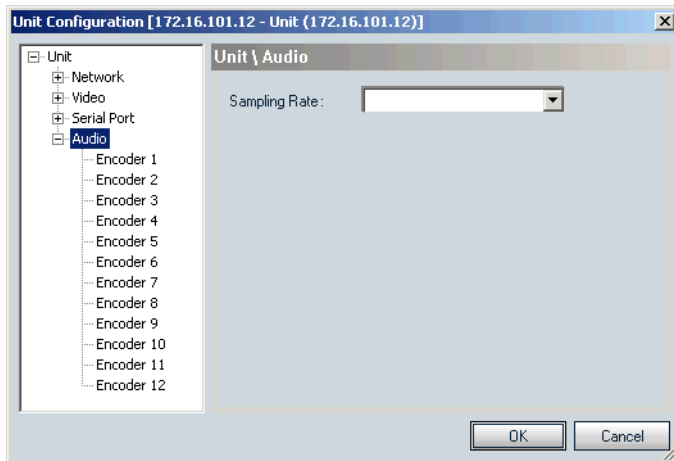
The only setting applicable to the complete audio functionality is:

- **Sampling Rate**—The rate (in kHz) at which the samples of the analog audio signal are taken in order to be converted into digital form.

To enable the audio functions in a point-to-point connection, see page 63. For details about the required physical connections for audio, refer to the user manual of your device.

## To change the sampling rate:

1. In the parameter tree, click **Audio**.



2. Change the setting.
3. Click **OK**.

# Audio\Encoder

The audio encoder (or *audio input*) parameters are:

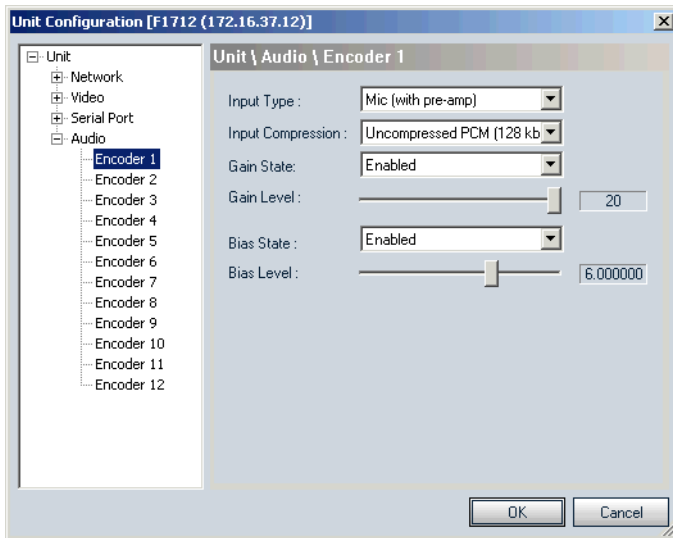
- Input Type—The type of your audio source. Two modes are supported:
  - Line-in
  - Mic (with pre-amp)
- Input Compression—The transfer mode for audio data. The following modes are available:
  - Uncompressed PCM (128 kbps)
  - ULAW (64 kbps)—default
  - GSM (16 kbps)
- Gain State—The indication of whether audio is amplified. Setting it to **Disabled** corresponds to mute.
- Gain Level—The amplification level. The level is taken into account only when the gain is enabled.
- Bias State—The indication of whether the bias is enabled on the device. This parameter applies to the S1708e series only.
- Bias Level—The level of voltage applied to a microphone to set its condition of operation. The bias level is taken into account only when the bias is enabled. The range of values is 0–9 volt.

## To change the audio encoder settings:

1. In the parameter tree, expand the **Audio** structure.

## 2: Setting Up the Edge Devices

### 2. Click **Encoder**.



### 3. Change the desired settings.

### 4. Click **OK**.

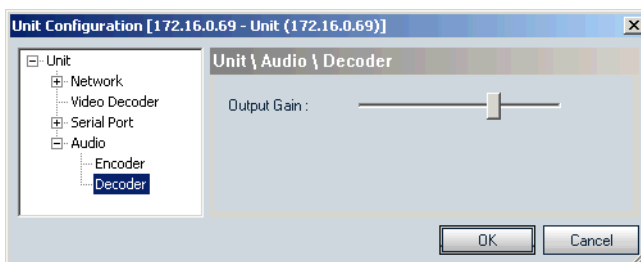
## Audio\Decoder

The audio decoder (or *audio output*) parameter is:

- Output Gain—The amplification level.

### To change the audio decoder setting:

1. In the parameter tree, expand the **Audio** structure.
2. Click **Decoder**.



### 3. Change the setting.



4. Click **OK**.

## Performing a Batch Network Configuration

You can configure the IP network settings of a batch of devices belonging to the same subnet in a single operation. For more information about these settings, see page 19.

Two methods are available to set the IP addresses: DHCP or manual. For more details on DHCP, see Appendix A on page 71.

### To perform a batch network configuration:

1. In the Units box, hold down the **Ctrl** key while selecting the devices to be configured.
2. Right-click in the selection, then choose **Batch Network Configuration** from the contextual menu.

The Batch Network Configuration window appears.

3. To assign IP addresses with DHCP, check **Use DHCP**.

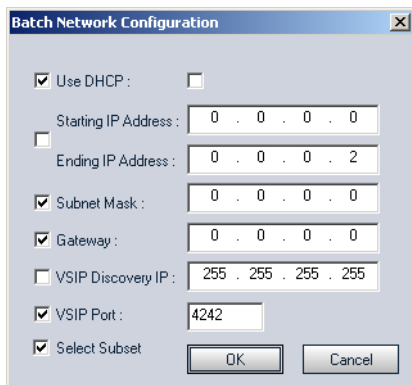
The next four fields become greyed out.

4. Change the fields as required.

In manual mode, you do not have to enter the ending IP address since it is automatically assigned according to the number of devices to configure: The address of each device is incremented by one.

## 2: Setting Up the Edge Devices

5. To change a subset of the settings, click **Select Subset**, then select the desired parameters. For example:



The Batch Network Configuration dialog box contains the following settings:

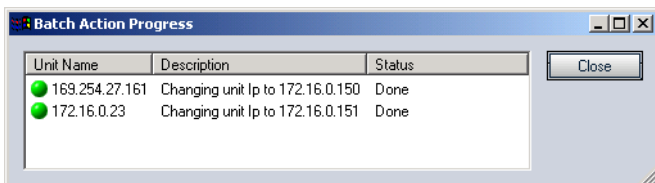
- ☒ Use DHCP : ☐
- Starting IP Address : 0 . 0 . 0 . 0
- ☐ Ending IP Address : 0 . 0 . 0 . 2
- ☒ Subnet Mask : 0 . 0 . 0 . 0
- ☒ Gateway : 0 . 0 . 0 . 0
- ☐ VSIP Discovery IP : 255 . 255 . 255 . 255
- ☒ VSIP Port : 4242
- ☒ Select Subset

Buttons: OK, Cancel

*Note: Do not clear the check box to the left of Use DHCP.*

6. To start the batch process, click **OK**.

The Batch Action Progress window appears, showing the status of each device.



The Batch Action Progress dialog box displays a table with the following data:

Unit Name	Description	Status
169.254.27.161	Changing unit ip to 172.16.0.150	Done
172.16.0.23	Changing unit ip to 172.16.0.151	Done

Buttons: Close

7. When all devices have been configured, click **Close**.

The devices will reboot with their new configuration.

# 3

## Updating Firmware

You can use SConfigurator to update the firmware of Nextiva edge devices.

*Warning: Firmware downgrade is not supported on any device. If you perform a downgrade, any problem encountered will not be covered by your product warranty.*

# Performing the Update

Updating a device retains its complete configuration.

Depending on the device, the available firmware update methods are:

Device	IP connection	Serial connection
S1000w	✓	✓
S1100w	✓	✓
S1500e	✓	✓
S1502e	✓	✓
S1504e	✓	
S1508e	✓	
S1600e	✓	✓
S1700e series	✓	
S1708e series	✓	
S2500e	✓	
S3100	✓	

You should take into consideration the following facts regarding firmware update using the IP network:

- It can be deactivated in the CLI. For more information, refer to the user manual of the device.
- Ensure that the IP link is stable before starting the procedure; therefore it is not recommended to perform it over the Internet.

If the firmware update over the IP network fails:

- S1000w, S1500e, S1502e, and S1600e: The device turns in *backup* mode, which requires a firmware update with a serial port connection (see page 50).
- S1100w: Do not reboot the device, and restart the procedure through the IP network as soon as possible. If you reboot the device before proceeding with the update procedure, it will stop responding and you will have to upgrade its firmware using the serial port.
- S1504e, S1508e, S1700e series, S1708 series, and S2500e: Restart the procedure. If the problem persists, move the device so that it is in the same IP subnet as the host computer.

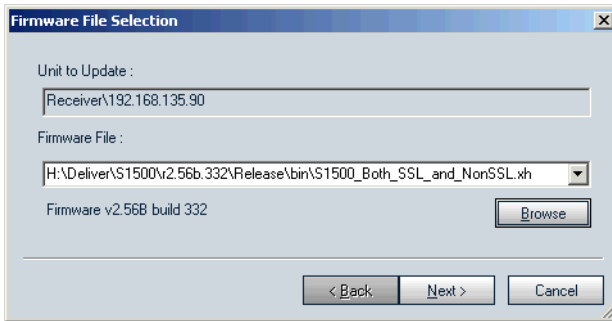
- S3100: The device turns in backup mode, which requires the update procedure to be restarted in a different context (see page 50).

The latest firmware files are available on the Verint Video Solutions web site (Firmware Upgrades section).

### To update firmware using an IP network connection:

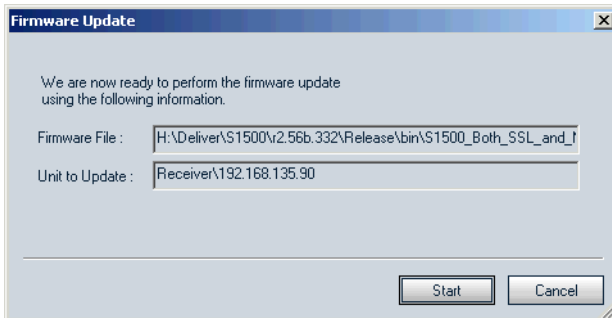
1. In the Firmware Update box of the Units tab, choose **Using an IP network connection**.
2. Click **Start**.

The Firmware File Selection window appears.



3. To open the desired firmware file, click **Browse**, then select it.
4. Click **Next**.

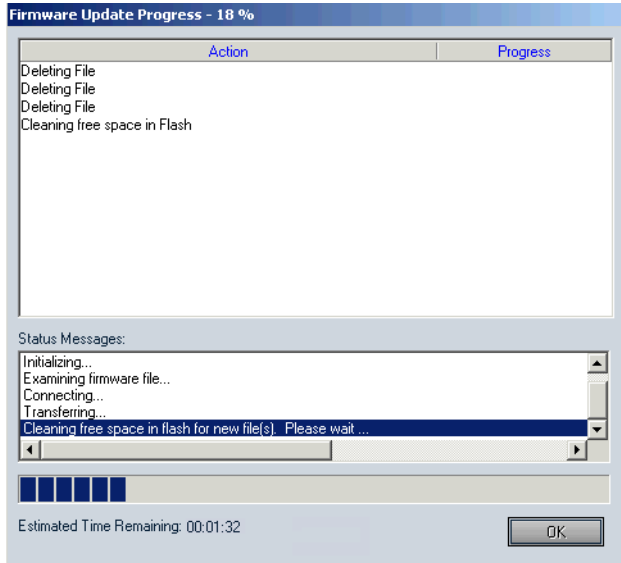
The Firmware Update window appears.



### 3: Updating Firmware

#### 5. Click **Start**.

The Firmware Update Progress window appears.



The update procedure may take several minutes to complete. For a list of status messages, see page 51.

#### **To restart the firmware update procedure on a bridge in backup mode:**

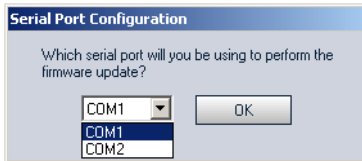
1. Move the S3100 device so that it is in the same IP subnet as the computer running SConfigurator.
2. Reboot the bridge.
3. In the Units tab, click **Discover**.
4. In the Units list, select the S3100 in backup mode.  
Such a device has the value *Backup* in its Type column.
5. Follow the update procedure described on page 49.

#### **To perform firmware update using a serial port connection:**

*Warning: SConfigurator needs a COM port to perform firmware update. You need to disable any program using this port prior to starting this procedure.*

1. Connect the host computer to the Nextiva device via the RS-232 serial port.
2. In the Firmware Update box of the Units tab, choose **Using a serial port connection**.
3. Click **Start**.

The Serial Port Configuration window appears.



4. Select the serial port to use, then click **OK**.  
The Firmware File Selection window appears.
5. To open the desired firmware file, click **Browse**, then select it.
6. Click **Next**.  
The Perform Update window appears.
7. Click **Start**.

The Firmware Update Progress window appears, displaying a progress bar and status messages.

The update procedure may take several minutes to complete.

## Firmware Update Messages

During firmware updates, many messages appear in the Firmware Update Progress window. The most frequent include:

**Another program is using the selected com port. Try again after the other program completes.** SConfigurator cannot open the communication port. Check that you are using the correct COM port or if it is being used by another application.

**Can't establish a connection to remote device via IP.**

SConfigurator cannot establish a connection with the device. The device may be powered down or disconnected from the network.

**Can't receive data via the serial port.** If this message appears before the update process, ensure that you have properly quit the CLI (by pressing **q** in the main menu). If this message appears during the process, you will need to reboot the device because it is in backup mode. Try performing another update using the serial port connection (for a video server) or the IP connection (for an outdoor wireless bridge). If the problem persists, contact Verint Video Solutions technical support.

**Communication established.** SConfigurator is now communicating with the device.

**Error: Invalid firmware file.** Select a valid file or ensure that the file exists. If the problem persists, contact Verint Video Solutions technical support to get a valid file.

**Firmware upload done.** The update process has been completed successfully.

**Firmware upload request sent.** SConfigurator has made a request to the Nextiva device for update.

**Invalid mih/smih file.** Select a valid file or ensure that the file exists. If the problem persists, contact Verint Video Solutions technical support to get a valid file.

**The firmware update failed.** A problem occurred during firmware update. The update process has not been completed successfully.



# 4

## Enabling Security

You can enable the SSL (Secure Sockets Layer) protocol in SConfigurator and in the SSL-enabled edge devices. Therefore, the connections between SConfigurator and a device or between two devices can be secure.

# Building a Secure System

SSL is a commonly used protocol for managing the security of message transmission on an IP network. SSL uses the public-and-private key encryption system from RSA, which also includes the use of a digital certificate; therefore, each SSL-enabled device comes with its own unique SSL certificate.

The SSL protocol secures the following data: I/O, serial port, and VSIP communication. It does not apply to audio and video transmission.

For increased security, Nextiva devices and SConfigurator use an SSL passkey. This passkey must be the same in all devices and in SConfigurator to establish a secure system. It is strongly recommended to change the default passkey (the empty string) prior to putting the devices in production.

On top of the SSL passkey, SConfigurator manages a list of devices it trusts. Therefore, fake devices with SSL certificates or hacked SConfigurator programs will not be able to break into your secure system.

## To build a secure system:

1. Create the list of devices that will work in the secure context (see page 7).  
  
This list is called the *trusted list*, and the enclosed devices, the *trusted devices*.
2. Set up the default secure VSIP connection between SConfigurator and a new device (see page 55).
3. For a video server, change its SSL passkey (see page 21) and VSIP port (see page 20).
4. For an S1100w wireless transmitter, change its wireless passkey (see page 29).
5. For an outdoor wireless bridge:
  - a. Change its SSL passkey (see page 21) and VSIP port (see page 20).
  - b. Change its wireless passkey (see page 29).
6. Add the device to the trusted list (see page 56).
7. Enable security in the device (see page 21).

8. Repeat steps step 2 to step 7 for each device to be part of the secure system, with the same SSL passkey and VSIP port.
9. Secure SConfigurator:
  - a. Change its VSIP port to the value assigned to the devices (see page 5).
  - b. Assign it the same SSL passkey as the devices, then enable its security (see page 7).

## Establishing the Default Secure VSIP Connection

When adding an SSL-enabled device in your environment, you need to create a secure VSIP connection to start the configuration process. To perform this type of connection, the device and SConfigurator must have the same VSIP port and the same SSL passkey.

VSIP (video services over IP) is a proprietary communication protocol used by SConfigurator and the devices on an IP network.

### **To establish the default secure VSIP connection between SConfigurator and an SSL-enabled device:**

1. In the Program Options window, set the SConfigurator VSIP port to 5510 and the SSL passkey to the empty string (see page 3).
2. On the edge device, set the VSIP port to 5510 (see page 20) and the SSL passkey to the empty string (see page 21).

If the device is new, it already has these factory default settings.

3. Discover the device (see page 10).

A secure VSIP connection is established between SConfigurator and the device.

# Adding a Device to the Trusted List

You can add a configured device to the list of devices SConfigurator SSL-trusts. If the trusted device list is not yet created, see page 7.

## To add the device to the trusted list:

1. In the Units box, right-click the device.
2. From the contextual menu, choose **Security > Trust Unit**.

The device is added to the trusted list. In the Units box, its value in the Trusted column turns to **Yes**.

# 5

## **Troubleshooting an Edge Device**

Here are frequently asked questions relative to security and device discovery.

### **What exactly is a secure VSIP connection? Is it the same as an SSL connection?**

A secure VSIP connection is a connection that is secured with SSL between SConfigurator and a device. This type of connection is also called *SSL* or *TCP-secured*.

To have a secure connection, you need the following prerequisites:

- The VSIP connection type must be TCP (the default value). If you change it manually to UDP in the CLI, no secure connection is possible.
- The SSL passkeys in the device and in SConfigurator must be the same.
- Obviously, SConfigurator and the device must have the same VSIP port (otherwise, the device will not be visible in the Units tab).

### **How come a secure VSIP connection can exist between a device and SConfigurator even if security is not enabled in them?**

Enabling security in SConfigurator and in a device only implies that they will not accept insecure connections anymore. As long as they share the same SSL passkey and the same VSIP port, their connection is secured with SSL.

### **I just enabled security on a device and added it to the trusted list. How come it becomes Unknown in the Units box and its VSIP connection turns to UDP instead of SSL?**

The VSIP connection between the device and SConfigurator is not secure because their SSL passkeys do not match. Remember that activating security on a device implies that it does not accept insecure connections anymore. As soon as the passkeys are the same, the VSIP connection will switch to SSL, and SConfigurator will be able to talk to the device and display its information.

**How come I can add a device without an SSL certificate in the trusted list?**

There is no link between SSL and the trusted list. You can include any device you want in the trusted list. However, if you enable security in SConfigurator, it will not be able to communicate with non-SSL devices anymore: The information on the devices will change to *Unknown* in the Units box.

**How come no devices appear in the Units box after I clicked the Discover button, even though I know there are many of them in the same LAN?**

The VSIP port is not the same in SConfigurator and in the devices.

**How come I do not see the new devices I just connected on my network, after clicking the Discover button?**

To be able to view the new devices, you must activate the Detect All Units on LAN setting in the Program Options (in the General tab). Since the IP addresses of such devices are always 169.254.X.Y, they are not in the same subnet as the computer running SConfigurator. You should also ensure that the VSIP port is the same in SConfigurator and in the devices.

However, you should not leave this setting activated after configuring your devices, since it slows down the discovery process on your network.

**How come I get an error message—specifying that the device cannot be located—after I entered the correct IP address of a device with the Add button?**

The VSIP port is not the same on SConfigurator and the device to be added.

**How come I cannot change the SSL passkey of a device in the Network configuration tab, even though I know that it has a digital certificate?**

The source of this problem is that the VSIP connection with SConfigurator is not secure. To solve the problem, you need to change the SSL passkey of the device through the CLI. As soon as the passkey is the same in the device and in SConfigurator, the VSIP connection becomes secure; you can then change the passkey in the Network tab.

**How come many devices become unknown after I activated security in SConfigurator?**

The following devices will become unknown in the Units box:

- Those without an SSL certificate
- Those not part of the trusted list
- Those not sharing the same SSL passkey



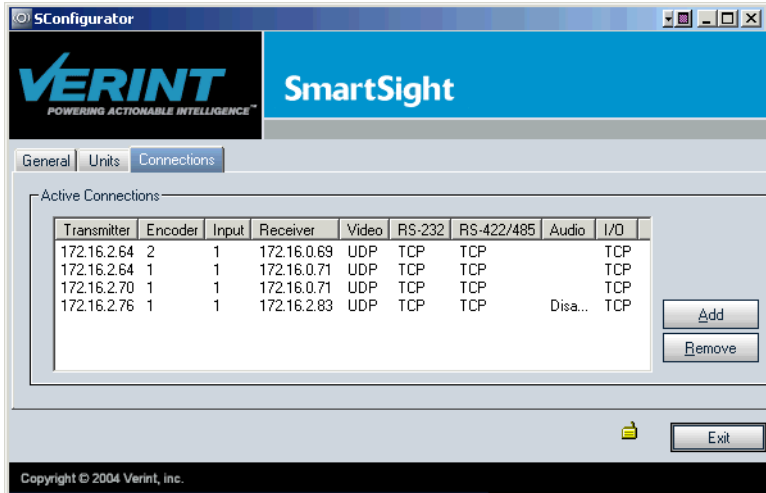
# 6

## **Managing Connections**

SConfigurator can manage point-to-point connections on the IP network. It allows you to add or remove connections between transmitter and receiver video servers, and to set the audio mode.

# Adding a Connection

You access the connection functions by clicking the Connections tab.



To create a connection between a transmitter and a receiver, both must be part of the Units box (in the Units tab).

*Note: You cannot create a connection with the S1504e, S1508e, S1708e, S1712e, and S1724e devices since they do not work in a point-to-point context.*

Before establishing a connection, you have to take into account the firmware versions of the involved transmitter and receiver:

- S1500e, S1502e, and S1600e—The two devices must have the same firmware version.
- S1100w, S1700e series, and S2500e—The receiver must be an S1500e-R running version 3.10.

The following video modes are available:

- UDP—The most effective mode, but without any error resilience (default).
- RTP—A video mode with bandwidth control, for error-prone links.
- TCP—The least effective mode, but totally error-free.

In addition to video, the connection can include audio, input/output (for example, alarms and events), and serial port data (like PTZ commands).

To include audio data in a connection, both devices must support this feature. Two transmission modes are available:

- In full duplex mode, audio will be transmitted and received simultaneously.
- The PTT/PTL (push-to-talk/push-to-listen) mode allows you to control audio communication. Audio data will be transmitted only if the PTT or PTL buttons are pressed.

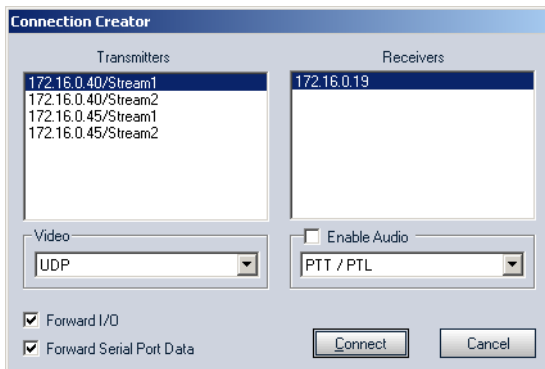
*Note: If you are assigning multiple connections on an S1500e series, S1600e or S1700e series, you have to create the one with audio last.*

For more information about audio, refer to the user manual of the device.

### To create a connection:

1. In the Connections tab, click **Add**.

The Connection Creator window appears.



2. Select a transmitter in the left column and a receiver in the right one.

In the Transmitters column, you have access to the two encoders of each input. The video stream is the same for both.

If you are using the web interface on an S1600e, S1700e, or S2500e device, use Stream2 for the point-to-point connection.

3. To disable I/O data transmission, clear **Forward I/O**.
4. To disable serial port data transmission, clear **Forward Serial Port Data**.

*Warning: You must clear this box if the transmitter is an S2500e IP camera, since it does not have a serial port.*

5. To enable audio between the devices, ensure that **Enable Audio** is checked, then select the audio mode.
6. Click **Connect**.

You should now have video on the monitor connected to the receiver device.

## Removing a Connection

You can remove an existing point-to-point connection between two devices. Removing a connection means that no more data will be transmitted between the two.

### To remove a connection:

1. In the Active Connections box of the Connections tab, select a connection, then click **Remove**.  
A confirmation window appears.
2. Click **OK**.

# 7

## **Accessing the CLI**

Each Nextiva edge device has a built-in command line interface (CLI) through which you can change its parameters, view statistics, and access advanced features. You access the CLI either through the SConfigurator console or Telnet.

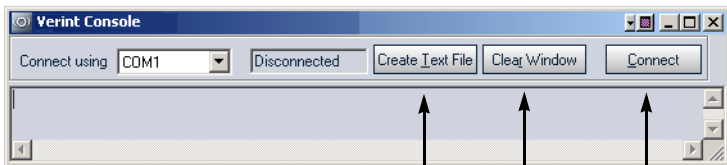
# SConfigurator Console

On video servers only, you can access the CLI with the SConfigurator console.

## To access the CLI of a device via the console:

1. Connect the device to a COM port of the computer using a serial cable.
2. In the General tab, click **Console**.

The Verint Console window appears.



To save the contents of the window to a text file

To delete the contents of the window

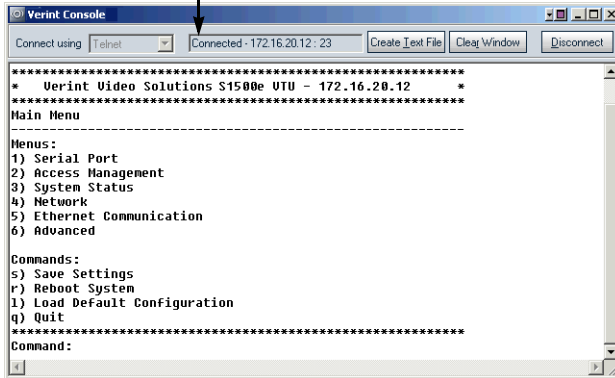
To start or stop the connection to the console

3. In the Connect using list, select the COM port used to communicate with the device.

#### 4. Click **Connect**.

The CLI main menu appears.

**Status of the connection: baud rate, data bits, parity, and stop bits**



The CLI has a timeout that is triggered after three minutes of inactivity. When the timeout occurs:

- You lose access to the command line.
- The "Thank you for using the Verint Video Solutions CLI." message appears at the command line.
- The Verint Console window becomes disabled.
- The Disconnect button switches to **Connect**.

#### 5. To reactivate the CLI after a timeout, click **Connect**.

#### 6. To work through the CLI menu structure, follow these guidelines:

- To execute a command or open a menu, type in the corresponding letter or number, then press **Enter**.
- To return to the previous menu, enter **p**.

#### 7. To end the CLI work session:

- a.** Save the settings by entering **s** at the main menu, then pressing **Enter**.
- b.** Exit the CLI by entering **q** at the main menu, then pressing **Enter**.

- c. Close the Verint Console window.

*Warning: Do not use the Disconnect button to exit the CLI. Clicking it does not free the RS-232 connection and does not save your settings.*

## Telnet

On all devices, you can use the Telnet terminal emulation program to access the CLI.

### To access the CLI of a device via Telnet:

- ◆ In the Units tab, select the desired device, then click **Telnet**.

The Verint Console window appears, displaying the last CLI menu accessed with Telnet. For more information about this window, see page 66.



# 8

## Aligning the Antenna

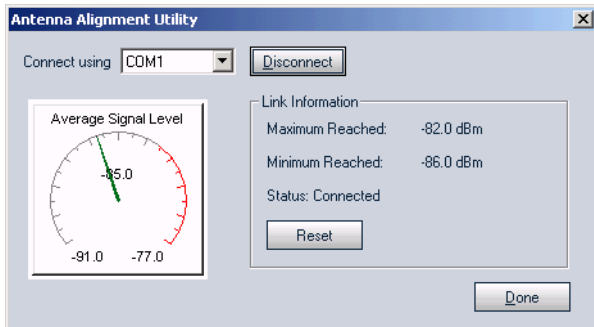
SConfigurator supplies a graphical environment helping you align the external antenna of an S1100w wireless transmitter or slave S3100 with that of its connected master bridge.

*Note: The antenna alignment utility works only with devices whose firmware release is 2.55 or higher.*

**To align the external antenna:**

1. In the General tab, click **Antenna Alignment**.

The Antenna Alignment Utility window appears.



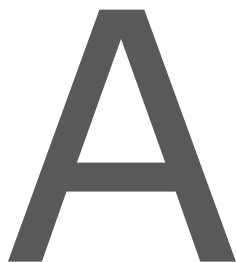
2. On an S1100w device:
  - Connect the device to a COM port of the host computer using a serial cable.
  - In the Connect using field, select the COM port, then click **Connect**.
3. On a slave S3100:
  - In the Connect using field, select **Telnet**, then click **Connect**.

The Telnet Connection window appears.
  - Enter the IP address of the slave device, then click **OK**.
4. Wait until the status becomes **Connected**.
5. Move the antenna so as to get the highest signal level possible (that is, the closest to 0 dBm).

The needle in the Average Signal Level dial moves to indicate the current radio signal (in dBm).

A red arc around the dial indicates the best values reached so far.

The dial automatically adjusts its range in real time to improve reading precision.
6. To recalibrate the dial and reset the minimum and maximum values reached, click **Reset**.
7. To exit, click **Done**.



# **DHCP Support and APIPA Service**

DHCP (Dynamic Host Configuration Protocol) allows devices and computers connected to a network to automatically get a valid IP configuration from a dedicated server.

The APIPA (Automatic Private IP Addressing) service, available on the Windows operating systems, enables a device to assign itself a temporary IP address.

## A: DHCP Support and APIPA Service

At startup, an edge device searches for a valid IP network configuration. The device requires this configuration prior to starting its functions. The network configuration for Nextiva devices consists of:

- An IP address
- A subnet mask
- A gateway

The device first looks in its local memory. If no configuration is found, it tries to contact a DHCP server. If DHCP configuration fails—if the device does not find a server or if it cannot get a configuration from it within one minute—the device assigns itself temporary network settings based on the APIPA service. This service allows a device to find a unique IP address until it receives a complete network configuration, either manually or from a DHCP server.

A device in APIPA mode does not reside on the same subnet as the other devices on the IP network; therefore, it may not be able to see them or be visible to them. Devices use the following temporary APIPA configuration:

- IP address: 169.254. \*. \*
- Subnet mask: 255.255.0.0
- Gateway: 169.254. \*. \*

The \*. \* portion is based on the MAC address of the device.

A device is in APIPA mode:

- The first time it boots up
- After receiving a duplicate IP address
- After a factory reset
- When the DHCP server does not have any available IP addresses

DHCP configuration is disabled:

- After a firmware upgrade
- After a factory reset

# Glossary

This glossary is common to the Nextiva line of products.

**Access Point** A device acting as a communication switch for connecting wireless edge devices to a wired LAN. Access points are mainly used with wireless transmitters to transfer wireless content onto the wired IP network.

**APIPA** (Automatic Private IP Addressing) A feature of Windows-based operating systems that enables a device to automatically assign itself an IP address when there is no Dynamic Host Configuration Protocol (DHCP) server available to perform that function. Also known as *AutoIP*.

**Bridge** A device linking a wireless network to a wired Ethernet network. The newest Nextiva bridge is the S3100.

**CCTV** (closed circuit television) A television system in which signals are not publicly distributed; cameras are connected to television monitors in a limited area such as a store, an office building, or on a college campus. CCTV is commonly used in surveillance systems.

**CIF** (common image format) A video format that easily supports both NTSC and PAL signals. Many CIF flavors are available, including CIF, QCIF, 2CIF, and 4CIF. Each flavor corresponds to a specific number of lines and columns per video frame.

**CLI** (command line interface) A textual user interface in which the user responds to a prompt by typing a command.

**Codec** (coder/decoder) A device that encodes or decodes a signal.

**Configuration Assistant** A proprietary graphical program used to configure and update the firmware of the S1100 edge devices.

**DCE** (data communication equipment) In an RS-232 communication channel, a device that connects to the RS-232 interface. Nextiva edge devices and modems are DCE.

**Decoder** See *Receiver*.

**DHCP** (Dynamic Host Configuration Protocol) A communication protocol that lets network administrators manage centrally and automate the assignment of Internet Protocol (IP) addresses in a network.

**DTE** (data terminal equipment) In an RS-232 communication channel, the device to which the RS-232 interface connects. Computers, switches, multiplexers, cameras, and keyboards are DTE.

**DVR** (digital video recorder) A device (usually a computer) that acts like a VCR in that it has the ability to record and play back video images. The DVR takes the feed from a camera and records it into a digital format on a storage device which is most commonly the hard drive.

**Encoder** See *Transmitter*.

**Ethernet** A local area network (LAN) architecture using a bus or star topology and supporting data transfer rates of 10 Mbps. It is one of the most widely implemented LAN standards. The 802.11 protocols are often referred to as "wireless Ethernet."

**Firmware** Software stored in read-only memory (ROM) or programmable ROM (PROM), therefore becoming a permanent part of a computing device.

**IP** (Internet Protocol) The network layer for the TCP/IP protocol suite widely used on Ethernet networks.

**LAN** (local area network) A computer network that spans a relatively small area. A LAN can connect workstations, personal computers, and surveillance equipment (like video servers). See also *WAN*.

**MPEG-4** A graphics and video lossy compression algorithm standard that is derived from MPEG-1, MPEG-2, and H.263. MPEG-4 extends these earlier algorithms with synthesis of speech and video, fractal compression, computer visualization, and artificial intelligence-based image processing techniques.

**Multicast** Communication between a single sender and multiple receivers on a network; the devices can be located across multiple subnets, but not through the Internet. Multicast is a set of protocols using UDP/IP for transport.

**nDVR** The SmartSight video management and storage software. This graphical product is used in conjunction with wired and wireless video servers.

**Nextiva** The Verint next generation, enterprise-class video management and analytics platform. Nextiva combines enterprise and security data with mission-critical video, leveraging existing investments in IT infrastructure, security, and business systems to enhance security and improve operational performance.

**NTSC** (National Television Standards Committee) The North American standard (525-line interlaced raster-scanned video) for the generation, transmission, and reception of television signals. In addition to North America, the NTSC standard is used in Central America, a number of South American countries, and some Asian countries, including Japan. Compare with *PAL*.

**NTP** (network time protocol) A protocol designed to synchronize the clocks of devices over a network.

**OSD** (on-screen display) Status information displayed on the video monitor connected to a receiver edge device.

**PAL** (Phase Alternation by Line) A television signal standard (625 lines, 50 Hz, 220V primary power) used in the United Kingdom, much of western Europe, several South American countries, some Middle East and Asian countries, several African countries, Australia, New Zealand, and other Pacific island countries. Compare with *NTSC*.

**PTL** (push-to-listen) In a two-way system, the communication mode in which the listener must push a button while listening.

**PTT** (push-to-talk) In a two-way system, the communication mode in which the talker must push a button while talking.

**PTZ Camera** (pan-tilt-zoom) An electronic camera that can be rotated left, right, up, or down as well as zoomed in to get a magnified view of an object or area. A PTZ camera monitors a larger area than a fixed camera.

**Receiver** A device converting a digital video signal into an analog form. Also called *decoder*.

**Repeater** A range extender for wireless links. The Nextiva repeater is made up of two S3100 bridges.

**RF** (radio frequency) Any frequency within the electromagnetic spectrum associated with radio wave propagation. When a modulated signal is supplied to an antenna, an electromagnetic field is created that is able to propagate through space. Many wireless technologies are based on RF field propagation.



**RS-232** A standard interface approved by the Electronic Industries Alliance (EIA) for connecting serial devices.

**RS-422** A standard interface approved by the Electronic Industries Alliance (EIA) for connecting serial devices, designed to replace the older RS-232 standard because it supports higher data rates and greater immunity to electrical interference.

**RS-485** An Electronics Industry Alliance (EIA) standard for multipoint communications.

**S1000 Series** The series of secure outdoor wireless video systems (one receiver and one transmitter per system). The series covers the 2.4 GHz band in North America and Europe and the 5 GHz band in North America. Starting with firmware release 3.20, the S1000 series is replaced by the S1100 edge devices.

**S1000w** The outdoor wireless video transmitter operating on the 2.4 GHz frequency band.

**S1100** The newest series of secure outdoor wireless video systems (one receiver and one transmitter per system) covering the 2.4 and 5 GHz bands in North America and Europe.

**S1100w** The multiband (2.4 and 5 GHz) outdoor wireless video transmitter operating in North America and Europe.

**S1500e Series** The series of wired video servers (receivers and transmitters) designed for video monitoring and surveillance over IP networks. The transmitters in the series offer from one to eight video inputs; the series proposes two receivers with one and four video outputs.

**S1600e** The high-resolution wired video server (receiver and transmitter) providing point-to-point analog extension with web access.

**S1700e Series** The newest series of wired video transmitters designed for video monitoring and surveillance over IP networks, offering DVD-quality video and power over Ethernet. The transmitter in the series offers one video input and web access.

**S1708e Series** The newest series of wired video transmitters designed for a variety of video monitoring and surveillance applications in which a high concentration of cameras terminates within the same area. The transmitters in the series offer 8, 12, or 24 video inputs.

**S2500e** The MPEG-4-compliant professional IP camera integrating a video camera and an Ethernet encoder in the same compact enclosure.

**S3100** The outdoor, wireless, digital video bridging device. It has many uses, including linking video servers (wireless or wired) to an Ethernet LAN and acting as a range extender.

**SConfigurator** A proprietary graphical program used to configure and update the firmware of video server and outdoor wireless bridge devices.

**Serial Port** An interface that can be used for serial communication, in which only one bit is transmitted at a time. A serial port is a general-purpose interface that can be used for almost any type of device.

**SSL** (Secure Sockets Layer) A commonly used protocol developed by Netscape for transmitting private documents via the Internet. SSL works by using a public key to encrypt data that is transferred over the SSL connection. The SSL protocol secures the following data: I/O, serial port, and VSIP communication; it does not apply to audio and video transmission.

**Transceiver** (transmitter/receiver) A device that both transmits and receives analog or digital signals.

**Transmitter** A device sending video signals captured with a connected camera or dome to a receiver. The transmitter converts the analog signal into a digital form before transmitting it. Also called *encoder*.

**Video Server** A device transmitting or receiving video signals through an IP network. The Nextiva wireless servers are the S1000w and S1100w devices; the wired servers are the S1500e series, S1600e, S1700e series, S1708e series devices.

**VSIP** (Video Services over IP) A proprietary communication protocol for sending messages between a computer and a Nextiva edge device, or between two devices.

**WAN** (wide area network) A computer network that spans a relatively large geographical area. Typically, a WAN consists of two or more local area networks (LANs).

**WEP** (Wired Equivalent Privacy) A security protocol for wireless local area networks (WLANs) defined in the 802.11b standard. It is designed to afford wireless networks the same level of protection as a comparable wired network.

**Wireless Cell** A group of wireless devices that communicate together on the same radio frequency channel and share the same wireless passkey.

**Wireless Transmission** A technology in which electronic devices send information to receivers using radio waves rather than wiring.



# Index

## A

- accessing
  - CLI 65–68
  - console 66
  - Telnet 68
- adding a connection 62
- address, IP. *See* IP address.
- alarm configuration 63
- aligning an antenna 69
- antenna alignment 69
- antenna gain 25
- APIPA device 11
- APIPA service 11, 71
- audio mode in a connection 63
- audio settings 42

## B

- backup mode 48
- band, frequency 23
- batch network configuration 45
- baud rate, serial port 41
- bias 43
- bit rate
  - RF. *See* wireless bit rate.
  - video 36
  - wireless. *See* wireless bit rate.
- bridge
  - available settings 15
  - See also* device.
- brightness 34
- broadcast detection method
  - in a device 20
  - in SConfigurator 5, 11

## C

- camera, IP. *See* video server.
- CD, Utilities vi
- certificate, SSL 54

- channel, RF
  - bridge 24
  - manual selection 24
  - S1000w 30
  - S1100w 24
- CIF resolution 37
- CLI (command line interface) 65–68
- client
  - changing the wireless bit rate 32
  - list of 31
- codec mode 38
- columns in the Units box 14
- COM port 66
- command line interface (CLI) 65–68
- common VSIP port 5, 11
- compatibility of firmware versions
  - in a connection 62
- compression, input 43
- computer requirements 2
- configuration
  - alarm 63
  - batch network 45
  - default 17
  - device 15–45
- connection
  - point-to-point 61–64
  - secure. *See* SSL connection.
  - serial port, for the CLI 66
  - SSL. *See* SSL connection.
  - transmitter and receiver 61–64
  - VSIP. *See* VSIP connection.
- Connections tab 61–64
- console, Verint 66
- contrast 34
- country of operation 17

## D

- decoder, video 40

## Index

- default value
  - resetting to 17
  - SSL passkey 54
  - VSIP port 5
- deleting a connection 64
- detecting devices. *See* discovery process.
- detection method. *See* discovery IP address.
- device
  - accessible to SConfigurator v APIPA 11
  - changing the name 17
  - configuring 15–45
  - configuring many at the same time 45
  - discovering 4, 10–13, 59
  - identifying 17
  - information to display 14
  - rebooting 16, 17
  - securing 21
  - troubleshooting 57–60
- DFS (Dynamic Frequency Selection) 17
- DHCP (Dynamic Host Configuration Protocol) 71
  - for a batch of devices 45
  - in a device 19
- digital SSL certificate 54
- discovery IP address
  - in a device 20
  - in SConfigurator 5, 11–12
- discovery process
  - all devices on LAN 4, 10–12, 59
  - many devices 10–13
  - new devices 4, 10–12, 59
  - one device 12, 13
- distance, maximum link 25
- downgrade of firmware 47
- duplex audio mode 63

## E

- emitting power 25
- encoder mode, video 38
- encoder settings 35–39
- encryption mechanism, WEP 30

- error messages during firmware update 51–52
- Ethernet settings
  - in a device 19
  - in SConfigurator 4

## F

- factory default configuration 17
- filter
  - IP 33
  - video 39
- firmware
  - compatibility of versions 62
  - downgrading 47
  - version, displayed 17
- firmware update
  - with IP link 48
  - messages 51–52
  - performing 47–51
  - preventing 21
  - with serial port 50
- forced bit rate 32
- frame rate 37
- frequency band 23
- frequency channel. *See* channel, RF.
- full duplex audio mode 63

## G

- gain
  - antenna 25
  - audio 43
- gateway, IP address 19
- general settings 17
- General tab 3–7, 66, 69–70
- GMT (Greenwich Mean Time) 22

## H

- hue 34

## I

- I/O data 63
- identifier for a pair of devices 30
- identifying a device 17
- I-frame 37
- information on devices 14

input compression 43  
input filter mode 39  
input type, audio 43  
input, video 34  
installation 2  
intra interval 37  
IP address  
    APIPA 71  
    computer 4  
    device 19  
    discovery 5  
    gateway 19  
    SConfigurator 4  
    subnet mask 19  
    temporary 71  
IP camera. *See* video server.  
IP filtering settings 33  
IP link  
    for firmware update 48  
    securing 53–56  
IP settings  
    in a device 19  
    in SConfigurator 4

**K**

key  
    WEP 30  
    wireless 26, 29

**L**

link distance, maximum 25  
link speed. *See* wireless bit rate.  
link status 31  
list of trusted devices  
    adding a device 56  
    creating 6  
    indicator in the Units box 14  
    troubleshooting 58  
loading default configuration 17  
lost device 11

**M**

MAC mode 23  
margin, minimum RF 26  
mask, subnet 19

master  
    list of clients and slaves 31  
    *See also* bridge.  
maximum link distance 25  
maximum quantizer 37  
messages, during firmware  
    update 51–52  
minimum RF margin 26  
mode  
    codec 38  
    MAC 23  
    RS-422/485 41  
multicast detection method  
    in a device 20  
    in SConfigurator 5, 12

**N**

name of device 17  
network configuration, batch 45  
network settings  
    for a batch of devices 45  
    in a device 19–33  
    in SConfigurator 4  
NTP (Network Time Protocol) 22  
NTSC 34

**O**

operating mode, serial port 41  
option. *See* settings.  
order, starting 25  
outdoor wireless bridge. *See*  
    bridge.  
output, video 40

**P**

PAL 34  
parameter. *See* settings.  
parity 41  
passkey  
    SSL. *See* SSL passkey.  
    wireless 26, 29  
point-to-point connection 61–64  
port  
    COM. *See* COM port.  
    serial. *See* serial port.  
    VSIP. *See* VSIP port.  
power, transmission 25

- preventing firmware update 21
- product type 14
- program settings 3–7
- PTT/PTL mode 63
- push-to-listen mode 63
- push-to-talk mode 63

## Q

- quantizer, maximum 37

## R

- radio frequency. *See* wireless settings.
- radio transmission power 25
- rate control, video 37
- rebooting the device 16, 17
- receiver-specific settings 40
- removing a connection 64
- requirements, computer 2
- reserved VSIP ports 5
- reset to factory default 17
- resolution, video 37
- RF (radio frequency). *See* wireless settings.
- role of the device 23
- RS-232 settings 40
- RS-422/485 settings 40

## S

- S1000w. *See* video server.
- S1100, configuration context 16
- S1100w
  - aligning the antenna 69
  - changing the RF wireless rate 32
  - configuration context 16
  - See also* video server.
- S1500e series
  - configuration context 16
  - See also* video server.
- S1600e. *See* video server.
- S1700e series. *See* video server.
- S1708e series. *See* video server.
- S2500e. *See* video server.
- S3100. *See* bridge.
- saturation, video 35

- scenarios for device discovery 10–12
- SDCF 23
- Secure Sockets Layer. *See the SSL entries.*
- secure VSIP connection. *See* SSL connection.
- security
  - defined 53–56
  - in a device 21
  - indicator in the Units box 14
  - in SConfigurator 6
- sensitivity threshold 26
- serial port
  - data in a connection 63
  - for firmware update 50
  - method to access the CLI 66
  - settings 40
- server, video. *See* video server.
- service set identifier (SSID) 30
- settings
  - audio 42
  - filtering 33
  - IP filtering 33
  - network 19–33, 45
  - NTP 22
  - RF (radio frequency) 23–33
  - SConfigurator 3–7
  - serial port 40
  - SSL. *See* SSL settings.
  - system status 17
  - video decoder 40
  - video encoder 34–39
  - VSIP. *See* VSIP settings.
  - wireless 23–33
- single device, discovering 12, 13
- slave
  - aligning the antenna 69
  - changing the wireless bit rate 32
  - list of 31
  - See also* bridge.
- SmartSight Utilities CD vi
- SPCF 23
- speed of the wireless link. *See* wireless bit rate.
- SSID (service set identifier) 30
- SSL certificate 54



SSL connection  
     defined 55  
     indicator in the Units box 14  
     troubleshooting 58–60

SSL passkey  
     defined 54  
     in a device 21  
     in SConfigurator 6  
     troubleshooting 58–60

SSL security. *See* security.

SSL settings  
     in a device 21  
     in SConfigurator 6

standard, television display 34

starting order 25

starting SConfigurator 2

status messages during firmware  
     update 51–52

status, system 17

stream, video 34–39

subnet mask 19

support, technical x

system status settings 17

system time 22

## T

target frame rate 37

target video bit rate 36

TCP connection 58

technical support x

television display standard 34

Telnet 21, 68

temporary IP address 71

threshold, sensitivity 26

time, system 22

timeout, CLI 67

TPC (Transmit Power Control) 17

transmission distance,  
     maximum 25

transmission power 25

troubleshooting a device 57–60

trusted device list  
     adding a device 56  
     creating 6  
     indicator in the Units box 14  
     troubleshooting 58

type, device 14

## U

UDP connection 58

unicast detection method 12

Units tab 9–52

updating firmware  
     with IP link 48  
     messages 51–52  
     performing 47–51  
     preventing 21  
     with serial port 50

Utilities CD vi

## V

Verint console 66

Verint Video Solutions web site ix

version of firmware 17, 62

video bit rate 36

video decoder setting 40

video encoder settings 35–39

video feed filtering 39

video input 34

video mode in a connection 62

video output 40

video server  
     available settings 15  
     list of v  
     *See also* device.

video settings 34–40

VSIP connection  
     defined 14  
     secure 55  
     troubleshooting 58–60

VSIP port  
     common 5, 11  
     default 5  
     in the discovery process 10–12  
     reserved 5  
     troubleshooting 59  
     *See also* VSIP settings.

VSIP settings  
     in a device 20  
     in SConfigurator 5

## W

web site, Verint Video  
     Solutions ix

## Index

- WEP (Wired Equivalent Privacy)
  - key 30
- wired video server, list of v
- wireless bit rate
  - changing, for a client or slave 32
  - S1000w 30
  - S1100w 24
  - slave 24
- wireless bridge. *See* bridge.
- wireless link status 31
- wireless passkey 26, 29
- wireless settings
  - in a bridge 23–33
  - in an S1000w 30
  - in an S1100 23–33
  - in an S1100w 23–33
- wireless transmitter. *See* S1000w *and* S1100w.
- wireless video server, list of v

Verint Video Solutions  
1800 Berlier Street  
Laval (Quebec)  
Canada  
H7L 4S4

